KASPERSKY LAB

Kaspersky® Anti-Virus for Windows Workstations 6.0

USER GUIDE

KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

User Guide

© Kaspersky Lab
http://www.kaspersky.com

Revision date: July 2007

Table of Contents

CHAPTER 1. THREATS TO COMPUTER SECURITY 11
1.1. Sources of Threats 11
1.2. How threats spread 12
1.3. Types of Threats 14
1.4. Signs of Infection 17
1.5. What to do if you suspect infection 18
1.6. Preventing Infection 19

CHAPTER 2. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0 . 21
2.1. What's new in Kaspersky Anti-Virus for Windows Workstations 6.0 21
2.2. The elements of Kaspersky Anti-Virus for Windows Workstations Defense 24
2.2.1. Protection components 24
2.2.2. Virus scan tasks 26
2.2.3. Program tools 27
2.3. Hardware and software system requirements 28
2.4. Software packages 29
2.5. Support for registered users 30

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0 31
3.1. Installation procedure using the Installation Wizard 32
3.2. Setup Wizard 36
3.2.1. Using objects saved with Version 5.0 36
3.2.2. Activating the program 37
3.2.2.1. Selecting a program activation method 37
3.2.2.2. Entering the activation code 38
3.2.2.3. Obtaining a key file 38
3.2.2.4. Selecting a license key file 38
3.2.2.5. Completing program activation 39
3.2.3. Selecting a security mode 39
3.2.4. Configuring update settings 40
3.2.5. Configuring a virus scan schedule 40

3.2.6. Restricting program access ... 41
3.2.7. Configuring Anti-Hacker settings ... 42
3.2.7.1. Determining a security zone's status ... 42
3.2.7.2. Creating a list of network applications ... 43
3.2.8. Finishing the Setup Wizard ... 44
3.3. Installing the program from the command prompt ... 44
3.4. Procedure for installing the Group Policy Object ... 45
3.4.1. Installing the program ... 45
3.4.2. Upgrading the program ... 46
3.4.3. Uninstalling the program ... 46
3.5. Upgrading from 5.0 to 6.0 ... 47

CHAPTER 4. PROGRAM INTERFACE ... 48
4.1. System tray icon ... 48
4.2. The context menu ... 49
4.3. Main program window ... 50
4.4. Program settings window ... 53

CHAPTER 5. GETTING STARTED ... 55
5.1. What is the protection status of the computer? ... 55
5.1.1. Protection indicators ... 56
5.1.2. Kaspersky Anti-Virus for Windows Workstations component status ... 59
5.1.3. Program performance statistics ... 60
5.2. How to scan your computer for viruses ... 61
5.3. How to scan critical areas of the computer ... 62
5.4. How to scan a file, folder or disk for viruses ... 62
5.5. How to train Anti-Spam ... 63
5.6. How to update the program ... 64
5.7. What to do if protection is not running ... 65

CHAPTER 6. PROTECTION MANAGEMENT SYSTEM ... 66
6.1. Stopping and resuming protection on your computer ... 66
6.1.1. Pausing protection ... 67
6.1.2. Stopping protection ... 68
6.1.3. Pausing / stopping protection components and tasks ... 68
6.1.4. Restoring protection on your computer ... 69
6.1.5. Shutting down the program ... 70

6.2. Types of malicious programs to be monitored 70
6.3. Creating a trusted zone 71
6.3.1. Exclusion rules 72
6.3.2. Trusted applications 77
6.4. Starting tasks under another profile 81
6.5. Configuring Scheduled Tasks and Notifications 82
6.6. Power options 84
6.7. Advanced Disinfection Technology 85

CHAPTER 7. FILE ANTI-VIRUS 86
7.1. Selecting a file security level 87
7.2. Configuring File Anti-Virus 88
7.2.1. Defining the file types to be scanned 88
7.2.2. Defining protection scope 91
7.2.3. Configuring advanced settings 92
7.2.4. Restoring default File Anti-Virus settings 95
7.2.5. Selecting actions for objects 95
7.3. Postponed disinfection 97

CHAPTER 8. MAIL ANTI-VIRUS 99
8.1. Selecting an email protection level 100
8.2. Configuring Mail Anti-Virus 102
8.2.1. Selecting a protected email group 102
8.2.2. Configuring email processing in Microsoft Office Outlook 104
8.2.3. Configuring email scans in The Bat! 105
8.2.4. Restoring default Mail Anti-Virus settings 107
8.2.5. Selecting actions for dangerous email objects 107

CHAPTER 9. WEB ANTI-VIRUS 110
9.1. Selecting the web security level 111
9.2. Configuring Web Anti-Virus 113
9.2.1. Setting a scan method 113
9.2.2. Creating a trusted address list 114
9.2.3. Restoring default Web Anti-Virus settings 115
9.2.4. Selecting responses to dangerous objects 116

CHAPTER 10. PROACTIVE DEFENSE 117
10.1. Proactive Defense settings 119

10.1.1. Activity control rules ... 121
10.1.2. Office Guard ... 124
10.1.3. Registry Guard ... 126
10.1.3.1. Selecting registry keys for creating a rule ... 128
10.1.3.2. Creating a Registry Guard rule ... 129

CHAPTER 11. ANTI-SPY ... 132
11.1. Configuring Anti-Spy ... 134
11.1.1. Creating Popup Blocker trusted address list ... 134
11.1.2. Banner ad blocking list ... 136
11.1.2.1. Configuring the standard banner ad blocking list ... 136
11.1.2.2. Banner ad white lists ... 137
11.1.2.3. Banner ad black lists ... 138
11.1.3. Creating an Anti-Dialer trusted number list ... 138

CHAPTER 12. PROTECTION AGAINST NETWORK ATTACKS ... 140
12.1. Selecting an Anti-Hacker security level ... 142
12.2. Application rules ... 143
12.2.1. Creating rules manually ... 145
12.2.2. Creating rules from template ... 146
12.3. Packet filtering rules ... 147
12.4. Fine-tuning rules for applications and packet filtering ... 149
12.5. Ranking rule priority ... 153
12.6. Rules for security zones ... 153
12.7. Firewall mode ... 156
12.8. Configuring the Intrusion Detection System ... 157
12.9. List of network attacks detected ... 158
12.10. Blocking and allowing network activity ... 161

CHAPTER 13. PROTECTION AGAINST UNWANTED E-MAIL ... 163
13.1. Selecting an Anti-Spam sensitivity level ... 165
13.2. Training Anti-Spam ... 166
13.2.1. Training Wizard ... 167
13.2.2. Training with outgoing emails ... 167
13.2.3. Training using your email client ... 168
13.2.4. Training using Anti-Spam reports ... 168
13.3. Configuring Anti-Spam ... 170

13.3.1. Configuring scan settings ... 170
13.3.2. Selecting spam filtration technologies ... 171
13.3.3. Defining spam and potential spam factors ... 172
13.3.4. Creating white and black lists manually ... 173
13.3.4.1. White lists for addresses and phrases ... 174
13.3.4.2. Black lists for addresses and phrases ... 175
13.3.5. Additional spam filtration features ... 177
13.3.6. Mail Dispatcher ... 179
13.3.7. Actions for spam ... 180
13.3.8. Configuring spam processing in Microsoft Office Outlook ... 180
13.3.9. Configuring spam processing in Outlook Express (Windows Mail) ... 183
13.3.10. Configuring spam processing in The Bat! ... 184

CHAPTER 14. SCANNING FOR VIRUSES ON THE COMPUTER ... 187
14.1. Managing virus scan tasks ... 188
14.2. Creating a list of objects to scan ... 188
14.3. Creating virus scan tasks ... 190
14.4. Configuring virus scan tasks ... 191
14.4.1. Selecting a security level ... 192
14.4.2. Specifying the types of objects to scan ... 193
14.4.3. Restoring default scan settings ... 195
14.4.4. Selecting actions for objects ... 196
14.4.5. Additional virus scan settings ... 198
14.4.6. Setting up global scan settings for all tasks ... 199

CHAPTER 15. TESTING KASPERSKY ANTI-VIRUS FEATURES ... 200
15.1. The EICAR test virus and its variations ... 200
15.2. Testing File Anti-Virus ... 202
15.3. Testing Virus scan tasks ... 203

CHAPTER 16. PROGRAM UPDATES ... 205
16.1. Starting the Updater ... 206
16.2. Rolling back to the previous update ... 207
16.3. Creating update tasks ... 207
16.4. Configuring update settings ... 208
16.4.1. Selecting an update source ... 209
16.4.2. Selecting an update method and what to update ... 211

16.4.3. Configuring connection settings ... 213
16.4.4. Update distribution ... 215
16.4.5. Actions after updating the program ... 216

CHAPTER 17. ADVANCED OPTIONS ... 217
17.1. Quarantine for potentially infected objects ... 218
17.1.1. Actions with quarantined objects ... 219
17.1.2. Setting up Quarantine ... 221
17.2. Backup copies of dangerous objects ... 222
17.2.1. Actions with backup copies ... 222
17.2.2. Configuring Backup settings ... 224
17.3. Reports ... 224
17.3.1. Configuring report settings ... 227
17.3.2. The *Detected* tab ... 227
17.3.3. The *Events* tab ... 228
17.3.4. The *Statistics* tab ... 229
17.3.5. The *Settings* tab ... 230
17.3.6. The *Macros* tab ... 231
17.3.7. The *Registry* tab ... 232
17.3.8. The *Phishing Sites* tab ... 233
17.3.9. The *Popup Windows* tab ... 233
17.3.10. The *Banner Ads* tab ... 234
17.3.11. The *Dial Attempts* tab ... 235
17.3.12. The *Network Attacks* tab ... 235
17.3.13. The *Banned Hosts* tab ... 236
17.3.14. The *Application Activity* tab ... 237
17.3.15. The Packet Filtering tab ... 237
17.3.16. The *Established Connections* tab ... 238
17.3.17. The *Open Ports* tab ... 240
17.3.18. The *Traffic* tab ... 240
17.4. General information about the program ... 241
17.5. Managing licenses ... 242
17.6. Technical Support ... 244
17.7. Creating a monitored port list ... 245
17.8. Checking encrypted connections ... 247
17.9. Configuring the Kaspersky Anti-Virus for Windows Workstations interface ... 249
17.10. Rescue Disk ... 250

17.10.1. Creating a rescue disk ... 251
17.10.2. Using the rescue disk ... 253
17.11. Using additional services ... 254
17.11.1. Kaspersky Anti-Virus for Windows Workstations event notifications ... 254
17.11.1.1. Types of events and notification delivery methods ... 255
17.11.1.2. Configuring email notification ... 257
17.11.1.3. Configuring event log settings ... 258
17.11.2. Self-Defense and access restriction ... 259
17.11.3. Resolving conflicts with other applications ... 261
17.12. Importing and exporting Kaspersky Anti-Virus for Windows Workstations settings ... 261
17.13. Resetting to default settings ... 262

CHAPTER 18. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT ... 264
18.1. Activating the application ... 265
18.2. Managing program components and tasks ... 266
18.3. Anti-virus scans ... 269
18.4. Program updates ... 273
18.5. Rollback settings ... 274
18.6. Exporting settings ... 275
18.7. Importing settings ... 276
18.8. Starting the program ... 276
18.9. Stopping the program ... 276
18.10. Obtaining a Trace File ... 277
18.11. Viewing Help ... 277
18.12. Return codes from the command line interface ... 278

CHAPTER 19. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM ... 279
19.1. Modifying, repairing, and removing the program using Installation Wizard ... 279
19.2. Uninstalling the program from the command prompt ... 281

CHAPTER 20. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT ... 283
20.1. Administering the application ... 285
20.1.1. Starting/stopping the application ... 286
20.1.2. Configuring application settings ... 287
20.1.3. Configuring specific settings ... 289

20.2. Managing tasks 290
20.2.1. Starting and stopping tasks 291
20.2.2. Creating tasks 292
20.2.2.1. Creating local tasks 292
20.2.2.2. Creating group tasks 294
20.2.2.3. Creating global tasks 294
20.2.3. Configuring specific task settings 295
20.3. Managing policies 296
20.3.1. Creating policies 296
20.3.2. Viewing and editing policy settings 298

CHAPTER 21. FREQUENTLY ASKED QUESTIONS 300

APPENDIX A. REFERENCE INFORMATION 302
A.1. List of files scanned by extension 302
A.2. Possible file exclusion masks 304
A.3. Possible threat exclusion masks 305
A.4. Overview of settings in *setup.ini* 306

APPENDIX B. KASPERSKY LAB 308
B.1. Other Kaspersky Lab Products 309
B.2. Contact Us 319

APPENDIX C. LICENSE AGREEMENT 321

CHAPTER 1. THREATS TO COMPUTER SECURITY

As information technology has rapidly developed and penetrated many aspects of human existence, so the number and range of crimes aimed at breaching information security has grown.

Cyber criminals have shown great interest in the activities of both state structures and commercial enterprises. They attempt to steal or disclose confidential information, which damages business reputations, disrupts business continuity, and may impair an organization's information resources. These acts can do extensive damage to assets, both tangible and intangible.

It is not only big companies who are at risk; individual users can also be attacked. Criminals can gain access to personal data (for instance, bank account and credit card numbers and passwords), or cause a computer to malfunction. Some types of attacks can give hackers complete access to a computer, which can then be used as part of a “zombie network” of infected computers to attack servers, send out spam, harvest confidential information, and spread new viruses and Trojans.

In today’s world, it is widely acknowledged that information is a valuable asset that should be protected. At the same time, information must be accessible to those who legitimately require it (for instance, employees, clients and partners of a business). Hence, the need to create a comprehensive information security system, which must take account of all possible sources of threats, whether human, man-made, or natural disasters, and use a complete array of defensive measures, at the physical, administrative and software levels.

1.1. Sources of Threats

A person, a group of people, or phenomena unrelated to human activity can threaten information security. Following from this, all threat sources can be put into one of three groups:

- **The human factor**. This group of threats concerns the actions of people with authorized or unauthorized access to information. Threats in this group can be divided into:
    - *External*, including cyber criminals, hackers, internet scams, unprincipled partners, and criminal organizations.

  - *Internal*, including the actions of company staff and users of home PCs. Actions taken by this group could be deliberate or accidental.

- **The technological factor**. This threat group is connected with technical problems – use of obsolete or poor-quality software and hardware to process information. This can lead to equipment failure and often to data loss.

- **The natural-disaster factor**. This threat group includes the whole range of events caused by nature and independent of human activity.

All three threat sources must be accounted for when developing a data security protection system. This User Guide focuses on the area that is directly tied to Kaspersky Lab's expertise – external threats involving human activity.

1.2. How threats spread

As modern computer technology and communications tools develop, hackers have more opportunities for spreading threats. Let's take a closer look at them:

The Internet

The Internet is unique, since it is no one's property and has no geographical borders. In many ways, this has promoted the development of web resources and the exchange of information. Today, anyone can access data on the Internet or create their own webpage.

However, these very features of the worldwide web give hackers the ability to commit crimes on the Internet, and make the hackers difficult to detect and punish.

Hackers place viruses and other malicious programs on Internet sites and disguise them as useful freeware. Furthermore, scripts that run automatically when you open certain web pages can execute dangerous actions on your computer, including modifying the system registry, stealing personal data, and installing malicious software.

By using network technologies, hackers can attack remote PCs and company servers. These attacks can cause parts of your system to malfunction, or could provide hackers with complete access to your system and thereby to the information stored on it. They can also use it as part of a zombie network.

Lastly, since it became possible to use credit cards and e-money through the Internet in online stores, auctions, and bank homepages, online scams have become increasingly common.

Intranet

Your intranet is your internal network, specially designed for handling information within a company or a home network. An intranet is a unified space for storing, exchanging, and accessing information for all the computers on the network. This means that if one computer on the network is infected, the others are at great risk of infection. To avoid such situations, both the network perimeter and each individual computer must be protected.

Email

Since the overwhelming majority of computers have email client programs installed, and since malicious programs exploit the contents of electronic address books, conditions are usually right for spreading malicious programs. The user of an infected computer might unknowingly send infected emails to friends or coworkers who in turn send more infected emails. For example, it is common for infected file documents to go undetected when distributed with business information via a company's internal email system. When this occurs, more than a handful of people are infected. It might be hundreds or thousands of company workers, together with potentially tens of thousands of subscribers.

Beyond the threat of malicious programs lies the problem of electronic junk email, or spam. Although not a direct threat to a computer, spam increases the load on email servers, eats up bandwidth, clogs up the user's mailbox, and wastes working hours, thereby incurring financial harm.

In addition, hackers have begun using mass mailing programs and social engineering methods to convince users to open emails, or click on a link to certain websites. It follows that spam filtration capabilities are valuable for several purposes: to stop junk email; to counteract new types of online scans, such as phishing; to stop the spread of malicious programs.

Removable storage media

Removable media (floppies, CD-ROMs, and USB flash drives) are widely used for storing and transmitting information.

Opening a file that contains malicious code and is stored on a removable storage device can damage data stored on the local computer and spread the virus to the computer's other drives or other computers on the network.

1.3. Types of Threats

There are a vast number of threats to computer security today. This section will review the threats that are blocked by Kaspersky Anti-Virus for Windows Workstations.

Worms

This category of malicious programs spreads itself largely by exploiting vulnerabilities in computer operating systems. The class was named for the way that worms crawl from computer to computer, using networks and email. This feature allows worms to spread themselves very rapidly.

When a worm penetrates a computer, it scans for the network addresses of other computers that are locally accessible, and sends a burst of self-made copies to these addresses. In addition, worms often utilize data from email client address books. Some of these malicious programs occasionally create working files on system disks, but they can run without any system resources except RAM.

Viruses

Viruses are programs that infect other files, adding their own code to them to gain control of the infected files when they are opened. This simple definition explains the fundamental action performed by a virus – *infection*.

Trojans

Trojans are programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, and so on. This class of malicious program is not a virus in the traditional sense of the word, because it does not infect other computers or data. Trojans cannot break into computers on their own. They are spread by hackers, who disguise them as regular software. The damage that they inflict can greatly exceed that done by traditional virus attacks.

Recently, worms have been the commonest type of malicious program damaging computer data, followed by viruses and Trojans. Some malicious programs combine features of two or even three of these classes.

Adware

Adware comprises programs that are included in software, unknown to the user, which is designed to display advertisements. Adware is usually built into software that is distributed free. The advertisement is situated in the program interface. These programs also frequently collect personal data on the user and send it back to their developer, change browser

settings (start page and search pages, security levels, etc.) and create traffic that the user cannot control. This can lead to a security breach and to direct financial losses.

Spyware

This software collects information about a particular user or organization without their knowledge. Spyware often escapes detection entirely. In general, the goal of spyware is to:

- Trace user actions on a computer;
- Gather information on the contents of your hard drive; in such cases, this usually involves scanning several directories and the system registry to compile a list of software installed on the computer;
- Gather information on the quality of the connection, bandwidth, modem speed, etc.

Riskware

Riskware includes software that has not malicious features but could form part of the development environment for malicious programs or could be used by hackers as auxiliary components for malicious programs. This program category includes programs with backdoors and vulnerabilities, as well as some remote administration utilities, keyboard layout togglers, IRC clients, FTP servers, and all-purpose utilities for stopping processes or hiding their operation.

Another type of malicious program that is similar to adware, spyware, and riskware are programs that plug into your web browser and redirect traffic. The web browser will open different web sites than those intended.

Jokes

Joke software does not do any direct damage, but displays messages stating that damage has already been done or will be under certain conditions. These programs often warn the user of non-existent dangers, such as messages that warn of formatting the hard drive (although no formatting actually takes place) or detecting viruses in uninfected files.

Rootkits

These are utilities that are used to conceal malicious activity. They mask malicious programs to keep anti-virus programs from detecting them. Rootkits modify basic functions of the computer's operating system to hide both their own existence and actions that the hacker undertakes on the infected computer.

Other dangerous programs

These are programs created to, for instance, set up denial of service (DoS) attacks on remote servers, hack into other computers, and programs that are part of the development environment for malicious programs. These programs include hack tools, virus builders, vulnerability scanners, password-cracking programs, and other types of programs for cracking network resources or penetrating a system.

Hacker attacks

Hacker attacks can be initiated either by hackers or by malicious programs. They are aimed at stealing information from a remote computer, causing the system to malfunction, or gaining full control of the system's resources. You can find a detailed description of the types of attacks blocked by Kaspersky Anti-Virus for Windows Workstations in section 12.9, on pg. 158.

Some types of online scams

Phishing is an online scam that uses mass emailings to steal confidential information from the user, generally of a financial nature. Phishing emails are designed to resemble informative emails from banks and well-known companies to the greatest extent possible. These emails contain links to fake websites created by hackers to mimic the site of the legitimate organization. On this site, the user is asked to enter, for example, his credit card number and other confidential information.

Dialers to pay-per-use websites – type of online scam using unauthorized use of pay-per-use Internet services, which are commonly pornographic web sites. The dialers installed by hackers initiate modem connections from your computer to the number for the pay service. These phone numbers often have very high rates and the user is forced to pay enormous telephone bills.

Intrusive advertising

This includes popup windows and banner ads that open when using your web browser. The information in these windows is generally not of benefit to the user. Popup windows and banner ads distract the user from the task and take up bandwidth.

Spam

Spam is anonymous junk email, and includes several different types of content: adverts; political messages; requests for assistance; emails that ask one to invest large amounts of money or to get involved in pyramid schemes; emails aimed at stealing passwords and credit card numbers, and emails that ask to be sent to friends (chain letters).

Spam significantly increases the load on mail servers and the risk of loosing important data.

Kaspersky Anti-Virus for Windows Workstations uses two methods for detecting and blocking these threat types:

- *Reactive* – this method searches for malicious files using a threat signature database that is regularly updated. At least one virus infection is necessary to implement this method – in order to add threat signature to the database and distribute database update.
- *Proactive* – in contrast to reactive protection, this method is based not on analyzing the object's code but on analyzing its behavior in the system. This method is aimed at detecting new threats that are still not defined in the signatures.

By employing both methods, Kaspersky Anti-Virus for Windows Workstations provides comprehensive protection for your computer from both known and new threats.

Warning:

From this point forward, we will use the term "virus" to refer to malicious and dangerous programs. The type of malicious programs will only be emphasized where necessary.

1.4. Signs of Infection

There are a number of signs that a computer is infected. The following events are good indicators that a computer is infected with a virus:

- Unexpected messages or images appear on the screen, or unusual sounds are played;
- The CD/DVD-ROM tray opens and closes unexpectedly;
- The computer arbitrarily launches a program without your assistance;
- Warnings pop up on the screen about a program attempting to access the Internet, even though you initiated no such action;

There are also several typical traits of a virus infection through email:

- Friends or acquaintances tell you about messages from you that you never sent;
- Your inbox houses a large number of messages without return addresses or headers.

It must be noted that these signs can arise from causes other than viruses. For example, in the case of email, infected messages can be sent with your return address but not from your computer.

There are also indirect indications that your computer is infected:

- Your computer freezes or crashes frequently;
- Your computer loads programs slowly;
- You cannot boot up the operating system;
- Files and folders disappear or their contents are distorted;
- The hard drive is frequently accessed (the light blinks);
- The web browser program (e.g., Microsoft Internet Explorer) freezes or behaves unexpectedly (for example, you cannot close the program window).

In 90% of cases, these indirect systems are caused by malfunctions in hardware or software. Despite the fact that such symptoms rarely indicate infection, we recommend that, upon detecting them, you are recommended to run a complete scan of your computer (see 5.2 on pg. 61).

1.5. What to do if you suspect infection

If you notice that your computer is behaving suspiciously…

1. Don't panic! This is the golden rule: it could save you from losing important data.
2. Disconnect your computer from the Internet or local network, if it is on one.
3. If the computer will not boot from the hard drive (the computer displays an error message when you turn it on), try booting in safe mode or with the emergency operating system boot disk that you created when you installed the operating system.
4. Before doing anything else, back up your work on removable storage media (floppy, CD/DVD, flash drive, etc.).
5. Install Kaspersky Anti-Virus for Windows Workstations, if you have not done so already.
6. Update the program's threat signatures and application modules (see 5.6 on pg. 64). If possible, download the updates off the Internet from a

different, uninfected, computer, for instance at a friend's, an Internet café, or work. It is better to use a different computer since, when you connect an infected computer to the Internet, there is a chance that the virus will send important information to hackers or spread the virus to the addresses in your address book. That is why if you suspect that your computer has a virus, you should immediately disconnect from the Internet. You can also get threat signature updates on floppy disk from Kaspersky Lab or its distributors and update your signatures using the disk.

7. Select the security level recommended by the experts at Kaspersky Lab.
8. Start a full computer scan (see 5.2 on pg. 61).

1.6. Preventing Infection

Not even the most reliable and deliberate measures can provide 100% protection against computer viruses and Trojans, but following such a set of rules significantly lowers the likelihood of virus attacks and the level of potential damage.

One of the basic methods of battling viruses is, as in medicine, well-timed *prevention*. Computer prophylactics involve a rather small number of rules that, if complied with, can significantly lower the likelihood of being infected with a virus and losing data.

The basic safety rules are given below. By following them, you can avoid virus attacks.

Rule No. 1: *Use anti-virus software and Internet security programs*. To do so:

- Install Kaspersky Anti-Virus for Windows Workstations as soon as possible.
- Regularly update the program's threat signatures (see 5.6 on pg. 64). You should update the signatures several times per day during virus outbreaks. In such situations, the threat signatures on Kaspersky Lab's update servers are updated immediately.
- Select the security settings recommended by Kaspersky Lab for your computer. You will be protected constantly from the moment the computer is turned on, and it will be harder for viruses to infect your computer.
- Select the settings for a complete scan recommended by Kaspersky Lab, and schedule scans for at least once per week. If you have not installed Anti-Hacker, we recommend that you do so to protect your computer when using the Internet.

Rule No. 2: *Use caution when copying new data to your computer*.

- Scan all removable storage drives, for example floppies, CDs/DVDs, and flash drives, for viruses before using them (see 5.4 on pg. 62).
- Treat emails with caution. Do not open any files attached to emails unless you are certain that you were intended to receive them, even if they were sent by people you know.
- Be careful with information obtained through the Internet. If any web site suggests that you install a new program, be certain that it has a security certificate.
- If you are copying an executable file from the Internet or local network, be sure to scan it with Kaspersky Anti-Virus for Windows Workstations.
- Use discretion when visiting web sites. Many sites are infected with dangerous script viruses or Internet worms.

Rule No. 3: *Pay close attention to information from Kaspersky Lab*.

In most cases, Kaspersky Lab announces a new outbreak long before it reaches its peak. The likelihood of the infection in such a case is low, and once you download the threat signature updates, you will have plenty of time to protect yourself against the new virus.

Rule No. 4: *Do not trust virus hoaxes*, such as prank programs and emails about infection threats.

Rule No. 5: *Use the Windows Update tool* and regularly install Windows operating system updates.

Rule No. 6: *Buy legitimate copies of software from official distributors*.

Rule No. 7: *Limit the number of people who are allowed to use your computer*.

Rule No. 8: *Lower the risk of unpleasant consequences of a potential infection*:

- Back up data regularly. If you lose your data, the system can fairly quickly be restored if you have backup copies. Store distribution floppies, CDs, flash drives, and other storage media with software and valuable information in a safe place.
- Create a Rescue Disk (see 17.10 on pg. 250) that you can use to boot up the computer, using a clean operating system.

Rule No. 9: *Regularly inspect the list of installed programs on your computer*. To do so, open **Install/Remove Programs** in the **Control Panel**, or open the **Program Files** directory. You may discover software here that was installed on your computer without your knowledge, for example, while you were using the Internet or installing a different program. Programs like these are almost always potentially dangerous.

CHAPTER 2. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

Kaspersky Anti-Virus for Windows Workstations 6.0 heralds a new generation of data security products.

What really sets Kaspersky Anti-Virus for Windows Workstations 6.0 apart from other software, even from other Kaspersky Lab products, is its multi-faceted approach to data security.

2.1. What's new in Kaspersky Anti-Virus for Windows Workstations 6.0

Kaspersky Anti-Virus for Windows Workstations 6.0 has a new approach to data security. The program's main feature is that it combines and noticeably improves the existing features of all the company's products in one security solution. The program provides protection against viruses, spam attacks, hacker attacks, unknown threats, phishing, and rootkits.

You will no longer need to install several products on your computer for overall security. It is enough simply to install Kaspersky Anti-Virus for Windows Workstations 6.0.

Comprehensive protection guards all incoming and outgoing data channels. All of the program's components have flexible settings that enable Kaspersky Anti-Virus for Windows Workstations to adapt to the needs of each user. Configuration of the entire program can be done from one location.

Let's take a look at the new features in Kaspersky Anti-Virus for Windows Workstations.

New Protection Features

- Kaspersky Anti-Virus for Windows Workstations protects you both from known malicious programs, and from programs still unknown. Proactive Defense (see Chapter 10 on pg. 117) is the program's key advantage. It analyzes the behavior of applications installed on your computer,

monitoring changes to the system registry, tracking macros, and fighting hidden threats. The component uses a heuristic analyzer to detect and record various types of malicious activity, with which actions taken by malicious programs can be rolled back and the system can be restored to its state prior to the malicious activity.

- The program protects the computer against rootkits and dialers, blocks banner ads, popup windows, and malicious scripts downloaded from web pages, and detects phishing sites.
- File Anti-Virus technology has been improved to lower the CPU load and increase the speed of file scans. iChecker™ and iSwift™ help achieve this. By operating this way, the program rules out scanning files twice.
- The scan process now runs as a background task, enabling the user to continue using the computer. If there is a competition for system resources, the virus scan will pause until the user's operation is completed and then resumes at the point where it left off.
- Critical areas of the computer, which if infected would seriously affect data quality or security, are given their own separate task. This task can be configured to run automatically every time the system is started.
- Protection for email systems against malicious programs and spam has been significantly improved. The program scans these protocols for emails containing viruses and spam:
    - IMAP, SMTP, POP3, regardless of which email client you use
    - NNTP (virus scan only), regardless of the email client
    - Regardless of the protocol (MAPI, HTTP) when using plug-ins for MS Outlook and The Bat!
- Special plug-ins are available for the most common mail clients, such as Outlook, Microsoft Outlook Express (Windows Mail), and The Bat! These place email protection against both viruses and spam directly in the mail client.
- Anti-Spam now has a training mode, based around the iBayes algorithm, which learns by monitoring how you deal with email. It also provides maximum flexibility in configuring spam detection – for instance, you can create black and white lists of addressees and key phrases that mark email as spam.

  Anti-Spam uses a phishing database, which can filter out emails designed to obtain confidential financial information.
- The program filters inbound and outbound traffic, traces and blocks threats from common network attacks, and lets you use the Internet in Stealth Mode.

- When using a combination of networks, you can also define which networks to trust completely and which to monitor with extreme caution.
- The user notification function (see 17.11.1 on pg. 254) has been expanded for certain events that arise during program operation. You can select the method of notification yourselves for each of these event types: e-mails, sound notifications, pop-up messages.
- Scanning has been added for data transmitted across secure SSL connections.
- The program has added self-defense features, including protection against unauthorized remote administration tools and password-protected program settings. These features help keep malicious programs, hackers, and unauthorized users from disabling protection.
- You can also create a rescue disk, with which you can reboot your operating system after a virus outbreak and scan your computer for malicious code.
- Now the protection system has the option of centralized remote administration, using an added administration interfaced under Kaspersky Administration Kit.

New Program Interface Features

- The new Kaspersky Anti-Virus for Windows Workstations interface makes the program's functions clear and easy to use. You can also change the program's appearance by using your own graphics and color schemes.
- The program regularly provides you with tips as you use it: Kaspersky Anti-Virus for Windows Workstations displays informative messages on the level of protection, accompanies its operation with hints and tips, and includes a thorough Help section.

New Program Update Features

- This version of the program debuts our improved update procedure: Kaspersky Anti-Virus automatically checks the update source for updates. If it finds new updates, Anti-Virus downloads them and installs them on the computer.
- The program downloads updates incrementally, ignoring files that have already been downloaded. This lowers the download traffic for updates by up to 10 times.
- Updates are downloaded from the most efficient source.
- You can choose not to use a proxy server, by downloading program updates from a local source. This noticeably reduces the traffic on the proxy server.

- The program has an update rollback feature that can return to the previous version of the signatures, if the threat signatures are damaged or there is an error in copying.
- A tool has been added to Updater that copies updates to a local folder to give other computers on the network access to them. This cuts down on Internet traffic.

2.2. The elements of Kaspersky Anti-Virus for Windows Workstations Defense

Kaspersky Anti-Virus for Windows Workstations is designed with the sources of threats in mind. In other words, a separate program component deals with each threat, monitoring it and taking the necessary action to prevent malicious effects of that threat on the user's data. This makes the Security Suite flexible, with user-friendly options for each of the components to fit the needs of a specific user or a business as a whole.

Kaspersky Anti-Virus for Windows Workstations includes:

- Protection Components (see 2.2.1 on pg. 24) that comprehensively defend all channels of data transmission and exchange on your computer in real-time mode.
- Virus Scan Tasks (see 2.2.2 on pg. 26) that virus-check the computer's memory and file system, as individual files, folders, disks, or regions.
- Support Tools (see 2.2.3 on pg. 27) that provide support for the program and extend its functionality.

2.2.1. Protection components

These protection components defend your computer in real time:

File Anti-Virus

A file system can contain viruses and other dangerous programs. Malicious programs can remain inactive in your file system for years after one day being copied from a floppy disk or from the Internet, without showing themselves at all. But you need only act upon the infected file, and the virus is instantly activated.

File Anti-virus is the component that monitors your computer's file system. It scans all files that are being opened, executed or saved on your computer and all connected disk drives. Each time a file is accessed, Kaspersky Anti-Virus intercepts it and scans the file for known viruses. If a file cannot be disinfected for any reason, it will be deleted, with a copy of the file either saved in Backup (see 17.2 on pg. 222), or moved to Quarantine (see 17.1 on pg. 218).

Mail Anti-Virus

Email is widely used by hackers to spread malicious programs, and is one of the most common methods of spreading worms. This makes it extremely important to monitor all email.

The *Mail Anti-Virus* component scans all incoming and outgoing email on your computer. It analyzes emails for malicious programs, only granting the addressee access to the email if it is free of dangerous objects.

Web Anti-Virus

By opening various web sites on the Internet, you risk infecting your computer with viruses installed on it with scripts that are stored on the web pages. You also risk download a dangerous file to your computer.

Web Anti-Virus is specially designed to combat these risks, by intercepting and blocking scripts on web sites if they pose a threat, and by thoroughly monitoring all HTTP traffic.

Proactive Defense

With every new day, there are more and more malicious programs. They are becoming more complex, combining several types, and the methods they use to spread themselves change, they become harder and harder to detect.

To detect a new malicious program before it has time to do any damage, Kaspersky Lab has developed a special component, *Proactive Defense*. It is designed to monitor and analyze the behavior of all installed programs on your computer. Kaspersky Anti-Virus decides, based on the program's actions: is it potentially dangerous? Proactive Defense protects your computer both from known viruses and from new ones that have yet to be discovered.

Anti-Spy

Programs that display unwanted advertising (for example, banner ads and popup windows), programs that call numbers for paid Internet services without user authorization, remote administration and monitoring tools, joke programs, etc. have become increasingly common.

Anti-Spy traces and blocks these actions on your computer. For example, the component blocks banner ads and popup windows, blocks programs that attempt autodialing, and analyzes web pages for phishing content.

Anti-Hacker

Hackers will use any potential hole to invade your computer, whether it is an open port, data transmissions between computers, etc.

The *Anti-Hacker* component protects your computer while you are using the Internet and other networks. It monitors inbound and outbound connections, and scans ports and data packets.

Anti-Spam

Although not a direct threat to your computer, spam increases the load on email servers, fills up your email inbox, and wastes your time, thereby representing a business cost.

The *Anti-Spam* component plugs into your computer's email client program, and scans all incoming email for spam subject matter. The component marks all spam emails with a special header. Anti-Spam can be configured to process spam as you like (auto delete, move to a special folder, etc.).

2.2.2. Virus scan tasks

In addition to constantly monitoring all potential pathways for malicious programs, it is extremely important to periodically scan your computer for viruses. This is necessary to detect malicious programs that were not previously discovered by the program because, for instance, its security level was set too low.

Kaspersky Anti-Virus for Windows Workstations configures, by default, the following virus-scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses. This includes system memory, programs loaded on startup, boot sectors on the hard drive, and the *Microsoft Windows* system directories. The task aims to detect active viruses quickly without fully scanning the computer.

My Computer

Scans for viruses on your computer with a thorough inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses in all programs that are loaded automatically on startup, plus RAM and boot sectors on hard drives.

There is also the option to create other virus-scan tasks and create a schedule for them. For example, you can create a scan task for email databases once per week, or a virus scan task for the **My Documents** folder.

2.2.3. Program tools

Kaspersky Anti-Virus for Windows Workstations includes a number of support tools, which are designed to provide real-time software support, expanding the capabilities of the program and assisting you as you go.

Updater

In order to be prepared for a hacker attack, or to delete a virus or some other dangerous program, Kaspersky Anti-Virus for Windows Workstations needs to be kept up-to-date. The *Updater* component is designed to do exactly that. It is responsible for updating the Kaspersky Anti-Virus for Windows Workstations threat signatures and program modules.

The update distribution feature can save threat signature and application module updates retrieved from Kaspersky Lab update servers in a local folder. It then grants other computers on the network access to them to conserve on Internet bandwidth.

Data Files

Each protection component, virus search task, and program update creates a report as it runs. The reports contain information on completed operations and their results. By using the *Reports* feature, you will remain up-to-date on the operation of all Kaspersky Anti-Virus for Windows Workstations components. Should problems arise, the reports can be sent to Kaspersky Lab, allowing our specialists to study the situation in greater depth and help you as quickly as possible.

Kaspersky Anti-Virus for Windows Workstations sends all files suspected of being dangerous to a special *Quarantine* area, where they are stored in encrypted form to avoid infecting the computer. You can scan these objects for viruses, restore them to their previous locations, delete them, or manually add files to Quarantine. Files that are found not to be infected upon completion of the virus scan are automatically restored to their former locations.

The *Backup* area holds copies of files disinfected and deleted by the program. These copies are created in case you either need to restore the

files, or want information about their infection. These backup copies are also stored in an encrypted form to avoid further infection.

You can manually restore a file from Backup to the original location and delete the copy.

Rescue Disk

Kaspersky Anti-Virus for Windows Workstations can create a Rescue Disk, which provides a backup plan if system files are damaged by a virus attack and it is impossible to boot the operating system. By using the Rescue Disk in such a case, you can boot your computer and restore the system to the condition prior to the malicious action.

Support

All registered Kaspersky Anti-Virus users can take advantage of our technical support service. To learn where exactly you can get technical support, use the *Support* feature.

Using these links, you can go to a Kaspersky Lab user forum and a list of frequently asked questions that may help you resolve your issue. In addition, by completing the form on the site, you can send Technical Support a message on the error or failure in the operation of the application.

You will also be able to access Technical Support on-line, and, of course, our employees will always be ready to assist you with Kaspersky Anti-Virus by phone.

2.3. Hardware and software system requirements

For Kaspersky Anti-Virus for Windows Workstations 6.0 to run properly, your computer must meet these minimum requirements:

General Requirements:

- 50 MB of free hard drive space
- CD-ROM drive (for installing Kaspersky Anti-Virus for Windows Workstations 6.0 from an installation CD)
- Microsoft Internet Explorer 5.5 or higher (for updating threat signatures and program modules through the Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Intel Pentium 300 MHz processor or faster (or compatible)
- 64 MB of RAM

Microsoft Windows 2000 Professional (Service Pack 4 or higher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 or higher), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHz processor or compatible
- 128 MB of RAM

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) or faster (or compatible)
- 512 MB of RAM

2.4. Software packages

You can purchase the boxed version of Kaspersky Anti-Virus for Windows Workstations from our resellers, or download it from Internet shops, including the **eStore** section of www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with an installation CD containing the program files
- A license key, included with the installation package or on a special diskette, or an application activation code on the CD slip.
- A User Guide
- The end-user license agreement (EULA)

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Anti-Virus for Windows Workstations from an online store, you copy the product from the Kaspersky Lab website (**Downloads → Product Downloads**). You can download the User Guide from the **Downloads → Documentation** section.

You will be sent a license key or activation code by email after your payment has been received.

The End-User License Agreement is a legal agreement between you and Kaspersky Lab that specifies the terms on which you may use the software you have purchased.

Read the EULA through carefully.

If you do not agree with the terms of the EULA, you can return your boxed product to the reseller from whom you purchased it and be reimbursed for the amount you paid for the program. If you do so, the sealed envelope for the installation disk must still be sealed.

By opening the sealed installation disk, you accept all the terms of the EULA.

2.5. Support for registered users

Kaspersky Lab provides its registered users with an array of services to make Kaspersky Anti-Virus for Windows Workstations more effective.

When the program has been activated, you become a registered user and will have the following services available until the license expires:

- New versions of the program free of charge
- Consultation on questions regarding installation, configuration, and operation of the program, by phone and email
- Notifications on new Kaspersky Lab product releases and new viruses (this services is for users that subscribe to Kaspersky Lab news mailings)

Kaspersky Lab does not provide technical support for operating system use and operation, or for any products other than its own.

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

There are several ways to install Kaspersky Anti-Virus for Windows Workstations:

- Local Installation: install the application on a single host. Direct access to the host in question is required to run and complete the install. A local install may be performed in one of the two modes below:
    - an interactive install using the application Installation Wizard (see 3.1 on page 32); this mode requires user input for the install to proceed;
    - a non-interactive install run from the command line and not requiring any user input for the install to proceed (see 3.3, pg. 44).
- Remote Installation: install the application to networked computers remotely from an administrator workstation using:
    - the Kaspersky Administration Kit software suite (cf. Kaspersky Administration Kit Deployment Guide);
    - Microsoft Windows Server 2000/2003 group domain policies (see 3.4, pg. 45).

It is recommended that all running applications be closed prior to Kaspersky Anti-Virus installation (including a remote installation).

In the event that you already have Kaspersky Anti-Virus 5.0 installed, it will be removed and updated to Kaspersky Anti-Virus 6.0 when the installation procedure is run (see 3.5, pg. 47 for more detail). Updates to more recent builds (minor versions) within Kaspersky Anti-Virus 6.0 are transparent.

3.1. Installation procedure using the Installation Wizard

To install Kaspersky Anti-Virus for Windows Workstations on your computer, open the Windows Installer file on the installation CD.

Note:

Installing the program with an installer package downloaded from the Internet is identical to installing it from an installation CD.

An installation wizard will open for the program. Each window contains a set of buttons for navigating through the installation process. Here is a brief explanation of their functions:

- **Next** – accepts an action and moves forward to the next step of installation.
- **Back** – goes back to the previous step of installation.
- **Cancel** – cancels product installation.
- **Finish** – completes the program installation procedure.

Let's take a closer look at the steps of the installation procedure.

Step 1. Checking for the necessary system conditions to install Kaspersky Anti-Virus for Windows Workstations

Before the program is installed on your computer, the installer checks your computer for the operating system and service packs necessary to install Kaspersky Anti-Virus for Windows Workstations. It also checks your computer for other necessary programs and verifies that your user rights allow you to install software.

If any of these requirements is not met, the program will display a message informing you of the fault. You are advised to install any necessary service packs through **Windows Update**, and any other necessary programs, before installing Kaspersky Anti-Virus for Windows Workstations.

Step 2. Installation Welcome window

If your system fully meets all requirements, an installation window will appear when you open the installer file with information on beginning the installation of Kaspersky Anti-Virus for Windows Workstations.

To continue installation, click the **Next** button. You may cancel installation by clicking **Cancel**.

Step 3. Viewing the End-User License Agreement

The next window contains the End-User License Agreement which is made between you and Kaspersky Lab. Carefully read through it, and if you agree to all the terms of the agreement, select **I accept the terms of the License Agreement** and click the **Next** button. Installation will continue.

To cancel the installation click the **Cancel** button.

Step 4. Selecting an installation folder

The next stage of Kaspersky Anti-Virus for Windows Workstations installation determines where the program will be installed on your computer. The default path is:

- **<drive> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Workstations** – for 32-bit systems.
- **<drive> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Workstations** – for 64-bit systems.

You can specify a different folder by clicking the **Browse** button and selecting it in the folder selection window, or by entering the path to the folder in the field available.

Remember that if you enter the full path to the installation folder manually, its length must not exceed 200 characters or contain special characters.

To continue installation, click the **Next** button.

Step 5. Using Saved Installation Settings

In this step, you are prompted to specify whether you wish to use previously saved security settings, threat signatures, and Anti-Spam databases if these were in fact saved when a previous Kaspersky Anti-Virus 6.0 installation was removed from your computer.

Let's take a closer look at how to use the options described above.

If you have previously installed another version or build of Kaspersky Anti-Virus for Windows Servers on your computer and you saved its threat signatures when you uninstalled it, you can use it in the current version. To do so, check **Threat signatures**. The threat signatures included with the program installation will not be copied to the server.

To use protection settings that you configured and saved from a previous version, check **Protection settings.**

You are also advised to use the Anti-Spam base if you saved one when you uninstalled the previous version of the program. This way, you will not have to retrain Anti-Spam. To use the base that you already created, check **Anti-Spam base**.

Step 6. Selecting an installation type

In this stage, you select how much of the program you want to install on your computer. You have three options:

Complete. If you select this option, all Kaspersky Anti-Virus for Windows Workstations components will be installed. The installation will recommence with Step 8. .

Custom. If you select this option, you can select the program components that you want to install. For more, see Step 7. .

Anti-virus features. This option installs only the components that protect you against viruses. Anti-Hacker, Anti-Spam and Anti-Spy will not be installed.

To select a setup type, click the appropriate button.

Step 7. Selecting program components to install

This step occurs only if you select the **Custom** setup type.

If you selected Custom installation, you can select the components of Kaspersky Anti-Virus for Windows Workstations that you want to install. By default, all protection components are selected, as well as connector to the Administration Agent for remote administration via Kaspersky Administration Kit are selected for installation

To select the components you want to install, left-click the icon alongside a component name and select **Will be installed on local hard drive** from the opened menu. You will find more information on what protection a selected component provides, and how much disk space it requires for installation, in the lower part of the program installation window.

If you do not want to install a component, select **Entire feature will be unavailable** item from the context menu. Remember that by choosing not to install a component you deprive yourself of protection against a wide range of dangerous programs.

After you have selected the components you want to install, click **Next**. To return the list to the default programs to be installed, click **Reset**.

Step 8. Disabling the Microsoft Windows firewall

You will only take this step if you are installing the Anti-Hacker component of Kaspersky Anti-Virus for Windows Workstations on a computer with the built-in firewall enabled.

In this step, Kaspersky Anti-Virus for Windows Workstations asks you if you want to disable the Windows Firewall, since the Anti-Hacker component of Kaspersky Anti-Virus for Windows Workstations provides full firewall protection.

If you wish to use Anti-Hacker as your primary browsing security tool, click **Next**. The Windows Firewall will be disabled automatically.

If you want to use the Windows Firewall, select **Keep Windows Firewall enabled**. If you select this option, Anti-Hacker will be installed, but disabled to avoid program conflicts.

Step 9. Searching for other anti-virus programs

In this stage, the installer searches for other anti-virus products installed on your computer, including Kaspersky Lab products, which could raise compatibility issues with Kaspersky Anti-Virus for Windows Workstations.

The installer will display on screen a list of any such programs it detects. The program will ask you if you want to uninstall them before continuing installation.

You can select manual or automatic uninstall under the list of anti-virus applications detected.

To continue installation, click the **Next** button.

Step 10. Finishing installing your program

In this stage, the program will ask you to finish installing the program on your computer.

When initially installing Kaspersky Anti-Virus 6.0, we do not recommend deselecting **Enable Self-Defense before installation**. Having protection modules enable will allow the installation to be rolled back correctly if errors occur while installing the application. If you are attempting to install the application again, we recommend deselecting this checkbox.

If the application is installed remotely via **Windows Remote Desktop**, we recommend unchecking the flag **Enable Self-Defense before installation**. Otherwise the installation procedure might not complete or complete correctly.

To continue installation, click the **Next** button.

Warning!

When Kaspersky Anti-Virus components which intercept network traffic are being installed current network connections are broken. Most of them will be recovered in some period of time.

Step 11. Completing the installation procedure

The **Complete Installation** window contains information on finishing the Kaspersky Anti-Virus installation process.

To start the setup wizard, click **Next** (see 3.2, pg. 36).

If installation is completed successfully, you will need to restart your computer, and a message on the screen will tell you so.

3.2. Setup Wizard

The Kaspersky Anti-Virus for Windows Workstations 6.0 Setup Wizard starts after the program has finished installation. It is designed to help you configure the initial program settings to conform to the features and uses of your computer.

The Setup Wizard interface is designed like a standard Windows Wizard and consists of a series of steps that you can move between using the **Back** and **Next** buttons, or complete using the **Finish** button**.** The **Cancel** button will stop the Wizard at any point.

You can skip this initial settings stage when installing the program by closing the Wizard window. In the future, you can run it again from the program interface if you restore the default settings for Kaspersky Anti-Virus for Windows Workstations (see 17.3 on page 224).

3.2.1. Using objects saved with Version 5.0

This wizard window appears when you install the application on top of Kaspersky Anti-Virus 5.0. You will be asked to select what data used by version 5.0 you want to import to version 6.0. This might include quarantined or backup files or protection settings.

To use this data in Version 6.0, check the necessary boxes.

3.2.2. Activating the program

Before activating the program, make sure that the computer's system date settings match the actual date and time.

The program is activated by installing a license key that Kaspersky Anti-Virus will use to check for a license and to determine the expiration date for it.

The license key contains system information necessary for all the program's features to operate, and other information:

- Support information (who provides program support and where you can obtain it)
- Name, number, and expiration date of your license

3.2.2.1. Selecting a program activation method

Depending on whether you have a key for Kaspersky Anti-Virus or need to obtain one from the Kaspersky Lab server, you have several options for activating the program:

Activate using the activation code. Select this activation option if you have purchased the full version of the program and were provided with an activation code. Using this activation code you will obtain a key file providing access to the application's full functionality throughout the effective term of the license agreement.

Activate trial version. Select this activation option if you want to install the trail version of the program before making the decision to buy a commercial version. You will be given a free key valid for a term specified in the trial version license agreement.

Apply existing license key. Activate the application using a Kaspersky Anti-Virus 6.0 license key file.

Activate later. If you choose this option, you will skip the activation stage. Kaspersky Anti-Virus for Windows Servers 6.0 will be installed on your computer and you will have access to all program features except updates (you can only update the threat signatures once after installing the program).

The first two activation options use a Kaspersky Lab web server, which requires an Internet connection. Before activating, make sure to edit your network settings (see 16.4.3 on pg. 213) in the window that opens when you click **LAN settings** (if necessary). For more in-depth information on configuring network settings, contact your system administrator or ISP.

If you have no Internet connection when installing the program you can activate the application later (see 17.5 on pg. 242) using its interface or you can use Internet access of another computer to register at Kaspersky Lab Technical Support website and get the key using activation code

3.2.2.2. Entering the activation code

You must enter an activation code to activate the program. If you purchase the program through the Internet, you will receive the activation code by e-mail. If you purchase a boxed version of the program, you will find the activation code on the installation CD-ROM envelope.

The activation code is a sequence of numbers and letters separated by dashes into four sections of five characters each, no spaces. For example, 11AA1-11AAA-1AA11-1A111. Note that the code must be entered in Latin characters.

Enter your contact information in the lower part of the window: full name, e-mail address, and country and city of residence. This information might be requested to identify a registered user if, for example, a key is lost or stolen. If that were to happen, your contact information will enable you to obtain a new license key.

3.2.2.3. Obtaining a key file

The Settings Wizard connects to Kaspersky Lab servers and sends them your registration data (the activation code and personal information), which are inspected on the server.

If the activation code passes inspection, the Wizard receives a key file. If you install the demo version of the program, the Settings Wizard will receive a trial key file without an activation code.

The file received will be installed automatically to use the program and you will see an activation completion window with detailed information on the key being used.

If the activation code does not pass inspection, you will see a corresponding message on the screen. If this occurs, contact the software vendors from whom you purchased the program for information.

3.2.2.4. Selecting a license key file

If you have a license key file for Kaspersky Anti-Virus for Windows Workstations 6.0, the Wizard will ask if you want to install it. If you do, use the **Browse** button and select the file path for the key file with the *.key* extension in the file selection window.

After you have successfully installed the key, you will see information about the license in the lower part of the window: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the expiration date for the key.

3.2.2.5. Completing program activation

The Setup Wizard will inform you that the program has been successfully activated. It will also display information on the license key installed: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the expiration date for the key.

3.2.3. Selecting a security mode

In this window, the Settings Wizard asks you to select the security mode that the program will operate with:

Basic. This is the default setting and is designed for users who do not have extensive experience with computers or anti-virus software. It sets all the program's components to their recommended security levels and only informs the user of dangerous events, such as the detection of malicious code or the execution of dangerous actions.

Interactive. This mode provides more customized defense of your computer's data than Basic Mode. It can trace attempts to modify system settings, suspicious activity in the system, and unauthorized activity on the network.

Each of these activities could be initiated by malicious programs or be a standard activity for some of the programs you use on your computer. You will have to decide for each separate case whether those activities should be allowed or blocked.

If you choose this mode, specify in what contexts it should be used:

- ☑ **Enable Anti-Hacker Training Mode** – prompts user for confirmation when programs installed on your computer attempt to connect to certain network resources. You can either allow or block that connection, and configure an Anti-Hacker rule for that program. If you disable Training Mode, Anti-Hacker runs with minimal protection settings, meaning that it grants all applications access to network resources.
- ☑ **Enable Registry Guard** – prompts user for a response when attempts to modify system registry keys are detected.

If the application is installed on a computer running Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64, the interactive mode settings listed below will not be available.

Enable Extended Proactive Defense – analyzes all suspicious activity by applications in the system, including browsers opening with command line settings, injection into application processes, and window hook interceptors (by default, this option is not selected).

3.2.4. Configuring update settings

Your computer's security depends directly on updating the threat signatures and program modules regularly. In this window, the Setup Wizard asks you to select a mode for program updates, and to configure a schedule.

Automatically. Kaspersky Anti-Virus checks the update source for updates at specified intervals. During virus outbreaks, the check frequency may increase, and decrease when they are gone. If it finds new updates, Anti-Virus downloads them and installs them on the computer. This is the default setting.

Every 2 hours. Updates will run automatically according to the schedule created. You can configure the schedule by clicking **Edit**.

Manually. If you choose this option, you will run program updates yourself.

Note that the threat signatures and program modules included with the software may be outdated by the time you install the program. That is why we recommend downloading the latest program updates. To do so, click **Update now**. Then Kaspersky Anti-Virus for Windows Workstations will download the necessary updates from the update servers and will install them on your computer.

If you want to configure updates (set up network properties, select the resource from which updates will be downloaded, set up running task under a certain account or enable update distribution option), click **Settings**.

3.2.5. Configuring a virus scan schedule

Scanning selected areas of your computer for malicious objects is one of the key steps in protecting your computer.

When you install Kaspersky Anti-Virus for Windows Workstations, three default virus scan tasks are created. In this window, the Setup Wizard asks you to choose a scan task setting:

Startup objects

By default, Kaspersky Anti-Virus automatically scans Startup objects when it starts up. You can edit the schedule properties in another window by clicking **Change**.

Critical Areas

To automatically scan critical areas of your computer (system memory, Startup objects, boot sectors, Windows system folders) for viruses, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting for this automatic scan is disabled.

My Computer

For a full virus scan of your computer to run automatically, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting, for scheduled running of this task, is disabled. However, we recommend running a full virus scan of your computer immediately after installing the program.

3.2.6. Restricting program access

Kaspersky Anti-Virus gives you the option of password-protecting the program, since several people with different levels of computer literacy may use the same computer, and since malicious programs could potentially disable protection. Using a password can protect the program from unauthorized attempts to disable protecting or change settings.

To enable password protection, check **Enable password protection** and complete the **Password** and **Confirm password** fields.

Select the area below that you want password protection to apply to:

- **All operations (other than warning notifications)**. Request password if the user attempts any action with the program, except for responses to notifications on detection of dangerous objects.
- **Selected operations:**
  - **Saving program settings** – request password when a user attempts to save changes to program settings.
  - **Exiting the program** – request password if a user attempts to exit the program.
  - **Stopping / pausing protection components and virus scan tasks** – request password if user attempts to pause or fully disable any protection component or virus scan task.

3.2.7. Configuring Anti-Hacker settings

Anti-Hacker is the Kaspersky Anti-Virus for Windows Workstations component that guards your computer on local networks and the Internet. At this stage, the Setup Wizard asks you to create a list of rules that will guide Anti-Hacker when analyzing your computer's network activity.

3.2.7.1. Determining a security zone's status

In this stage, the Setup Wizard analyzes your computer's network environment. Based on its analysis, the entire network space is broken down into zones:

Internet – the World Wide Web. In this zone, Kaspersky Anti-Virus for Windows Workstations operates as a personal firewall. In doing so, default rules for packet filtering and applications regulate all network activity to ensure maximum security. You cannot change protection settings when working in this zone, other than enabling Stealth Mode on your computer for added safety.

Security zones – certain zones that mostly correspond with subnets that include your computer (this could be local subnets at home or at work). These zones are by default average risk-level zones. You can change the status of these zones based on how much you trust a certain subnet, and you can configure rules for packet filtering and applications.

All the zones detected will be displayed in a list. Each of them is shown with a description, their address and subnet mask, and the degree to which any network activity will be allowed or blocked by Anti-Hacker.

- **Internet**. This is the default status assigned to the Internet, since when you are connected to it, your computer is subjected to all potential threat types. This status is also recommended for networks that are not protected by any anti-virus programs, firewalls, filters, etc. When you select this status, the program ensures maximum security while you are using this zone, specifically:
    - blocking any network NetBios activity within the subnet
    - blocking rules for applications and packet filtering that allow NetBios activity within this subnet

  Even if you have created a shared folder, the information in it will not be available to users from subnetworks with this status. Additionally, if this status is selected for a certain subnetwork, you will not be able to access files and printers of this subnetwork.
- **Local Area Network**. The program assigns this status to the majority of security zones detected when it analyzes the computer's network

environment, except the Internet. It is recommended to apply this status to zones with an average risk factor (for example, corporate LANs). If you select this status, the program allows:

- any network NetBios activity within the subnet
- rules for applications and packet filtering that allow NetBios activity within this subnet

Select this status if you want to grant access to certain folders or printers on your computer, but want to block all other outside activity.

- **Trusted (allow all connections).** This status is given to networks that you feel are absolutely safe, so that your computer is not subject to attacks and attempts to gain access to your data while connected to it. When you are using this type of network, all network activity is allowed. Even if you have selected Maximum Protection and have created block rules, they will not function for remote computers from a trusted network.

You can use *Stealth Mode* for added security when using networks labeled **Internet**. This feature only allows network activity initiated from your computer, meaning that your computer becomes invisible to its surroundings. This mode does not affect your computer's performance on the Internet.

We do not recommend using Stealth Mode if you use your computer as a server (for example, a mail or HTTP server), as the computers that attempt to connect to the server will not see it as connected.

To change the status of a zone or to enable/disable Stealth Mode, select the zone from the list, and use the appropriate links in the **Rule description** box below the list. You can perform similar tasks and edit addresses and subnet masks in the **Zone Settings** window, which you can open by clicking **Edit**.

You can add a new zone to the list while viewing it. To do so, click **Find**. Anti-Hacker will search for available zones, and if it detects any, the program will ask you to select a status for them. In addition, you can add new zones to the list manually (if you connect your laptop to a new network, for example). To do so, use the **Add** button and fill in the necessary information in the **Zone Settings** window.

To delete a network from the list, click the **Delete** button.

3.2.7.2. Creating a list of network applications

The Setup Wizard analyzes the software installed on your computer and creates a list of applications that use network connections.

Anti-Hacker creates a rule to control network activity for each such application. The rules are applied using templates for common network applications, created at Kaspersky Lab and included with the software.

You can view the list of network applications and their rules in the Anti-Hacker settings window, which you can open by clicking **List**.

For added security, we recommend disabling DNS caching when using Internet resources. DNS caching drastically cuts down on the time your computer is connected to this valuable Internet resource; however, it is also a dangerous vulnerability, and by exploiting it, hackers can create data leaks that cannot be traced using the firewall. Therefore, to increase the degree of security for your computer, you are advised to disable DNS caching.

3.2.8. Finishing the Setup Wizard

The last window of the Wizard will ask if you want to restart your computer to complete the program installation. You must restart for Kaspersky Anti-Virus for Windows Workstations drivers to register.

Some program components will not work until you can restart.

3.3. Installing the program from the command prompt

To install Kaspersky Anti-Virus 6.0 for Windows Workstations, enter this at the command prompt:

```
msiexec / i <package_name>
```

The Installation Wizard will start (see 3.1 on pg. 32). Once the program is installed, you must restart the computer.

To install the application non-interactively (without running the Installation Wizard), enter:

```
msiexec /i <package_name> /qn
```

This option will require you to reboot your machine manually once the installation is complete. To perform an automatic reboot from the command line, enter:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Please note that an automatic reboot will occur in non-interactive mode (using the /qn key).

To install the application with an uninstall password, enter:

`msiexec /i <package_name> KLUNINSTPASSWD=******`, when performing an interactive installation;

`msiexec /i <package_name> KLUNINSTPASSWD=****** /qn`, when performing a non-interactive installation without system reboot;

`msiexec /i <package_name> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, when performing a non-interactive installation with system reboot;

If you install Kaspersky Anti-Virus in the noninteractive mode, you can access the file *setup.ini*, which contains the general settings for application installation (see A.4 on pg. 306), the configuration *install.cfg* (see 18.8 on pg. 276), and the license key file. Note that these files must be located in the same folder as the Kaspersky Anti-Virus installer package.

3.4. Procedure for installing the Group Policy Object

This feature is supported on computers running Microsoft Windows 2000 or higher.

Using **Group Policy Object Editor**, you can install, update, and uninstall Kaspersky Anti-Virus on enterprise workstations within the domain without using Kaspersky Administration Kit.

3.4.1. Installing the program

To install Kaspersky Anti-Virus:

1. Create a shared folder on the computer that is the domain controller and copy the Kaspersky Anti-Virus *.msi* installer package to it.

   You can also copy in the file *setup.ini*, which contains the general settings for application installation (see A.4 on pg. 306), the configuration *install.cfg* (see 18.7 on pg. 276), and the license key file.

2. Open the **Group Policy Object Editor** via MMC (for more detailed information on using Group Policy Object, consult help in Microsoft Windows Server).

3. Create a new package. To do so, from the console tree, select **Group Policy Object/ Computer Configuration/ Software Settings/**

Software installation and use the command **New**/ **Package** from the context menu.

In the window that opens, specify the path to the shared folder with the Anti-Virus installer (see 1). Select **Assign** from the **Select Deployment Method** dialog box and click **OK**.

The group policy will be enforced on each workstation the next time the computer is registered in the domain. Kaspersky Anti-Virus will then be installed on all computers.

3.4.2. Upgrading the program

To upgrade Kaspersky Anti-Virus:

1. Copy the installer package containing the Kaspersky Anti-Virus update in *.msi* format to the shared folder.
2. Open **Group Policy Object Editor** and created a new package using the steps given above.
3. Select the new package and select the **Properties** command from the context menu. In the package properties window, go to the **Upgrades** tab and specify the package that contains the installer for the previous version of Kaspersky Anti-Virus. To install the Kaspersky Anti-Virus upgrade and keep your protection settings, select a variant of upgrading the previous version.

The group policy will be enforced on each workstation the next time the computer is registered in the domain.

Note that Kaspersky Anti-Virus on computers running Microsoft Windows 2000 Professional cannot be upgraded using Group Policy Object Editor.

3.4.3. Uninstalling the program

To uninstall Kaspersky Anti-Virus:

1. Open **Group Policy Object Editor**.
2. To do so, from the console tree, select **Group Policy Object**/ Computer Configuration/ Software Settings/ Software installation.

   Select the Kaspersky Anti-Virus package from the list. Open the context menu and select the command **All Tasks**/ **Remove**.

In the **Remove Software** dialog box, select **Immediately uninstall the software from users and computers** for Kaspersky Anti-Virus to be uninstalled the next time a computer restarts.

3.5. Upgrading from 5.0 to 6.0

If Kaspersky Anti-Virus 5.0 for Windows Workstations is installed on your computer, you can upgrade it to Kaspersky Anti-Virus 6.0.

After you start the Kaspersky Anti-Virus 6.0 installation program, you will be given the choice of first uninstalling the already installed version 5.0. Once the uninstall process is complete, you must restart your computer, after which version 6.0 installation will run.

Warning!

When you upgrade Kaspersky Anti-Virus 5.0 to 6.0 from a password-protected network folder, version 5.0 will be uninstalled and the computer will be restarted without then installing version 6.0 of the application. This is because the installer program does not have access privileges to the network folder. To resolve this problem, only run the installer from a local folder.

CHAPTER 4. PROGRAM INTERFACE

Kaspersky Anti-Virus for Windows Workstations has a straightforward, user-friendly interface. This chapter will discuss its basic features:

- System tray icon (see 4.1 on pg. 48)
- Context menu (see 4.2 on pg. 49)
- Main window (see 4.3 on pg. 50)
- Program settings window (see 4.4 on pg. 53)

In addition to the main program interface, there are plug-ins for the following applications:

- Microsoft Office Outlook – virus scans (see 8.2.2 on pg. 104) and spam scans (see 13.3.8 on pg. 180)
- Microsoft Outlook Express (Windows Mail) (see 13.3.9 on pg. 183)
- The Bat! – virus scans (see 8.2.3 on pg. 105) and spam scans (see 13.3.10 on pg. 184)
- Microsoft Internet Explorer (see Chapter 11 on pg. 132)
- Microsoft Windows Explorer (see 14.2 on pg. 188)

The plug-ins extend the functionality of these programs by making Kaspersky Anti-Virus for Windows Workstations management and settings possible from their interfaces.

4.1. System tray icon

As soon as you install Kaspersky Anti-Virus for Windows Workstations, its icon will appear in the system tray.

The icon is an indicator for Kaspersky Anti-Virus for Windows Workstations functions. It reflects the state of protection and shows a number of basic functions performed by the program.

If the icon is active (color), this means that your computer is being protected. If the icon is inactive (black and white), this means that all protection components (see 2.2.1 on pg. 24) are disabled.

The Kaspersky Anti-Virus for Windows Workstations icon changes in relation to the operation being performed:

	Emails are being scanned.
	Scripts are being scanned.
	A file that you or some program is opening, saving, or running is being scanned.
	Kaspersky Anti-Virus for Windows Workstations threat signatures and program modules are being updated.
	An error has occurred in some Kaspersky Anti-Virus component.

The icon also provides access to the basics of the program interface: the context menu (see 4.2 on pg. 49) and the main window (see 4.3 on pg. 50).

To open the context menu, right-click on the program icon.

To open the Kaspersky Anti-Virus for Windows Workstations main window at the **Protection** section (this is the default first screen when you open the program), double-click the program icon. If you single-click the icon, the main window will open at the section that was active when you last closed it.

4.2. The context menu

You can perform basic protection tasks from the context menu (see Figure 1).

The Kaspersky Anti-Virus for Windows Workstations menu contains the following items:

Scan My Computer – launches a complete scan of your computer for dangerous objects. The files on all drives, including removable storage media, will be scanned.

Virus scan… – selects objects and starts scanning them for viruses. The default list contains a number of files, such as the **My Documents** folder, the Startup folder, email databases, all the drives on your computer, etc. You can add to the list, select files to be scanned, and start virus scans.

Figure 1. The context menu

Update – starts program modules and threat signatures update and install them on your computer.

Network Monitor – view the list of network connections established, open ports, and traffic.

Activate… – activate the program. You must activate your version of Kaspersky Internet Security to obtain registered user status which provides access to the full functionality of the application and Technical Support. This menu item is only available if the program is not activated.

Settings… – view and configure settings for Kaspersky Anti-Virus for Windows Workstations.

Open Kaspersky Anti-Virus – open the main program window (see 4.3 on pg. 50).

Pause Protection / Resume Protection – temporarily disable or enable protection components (see 2.2.1 on pg. 24). This menu item does not affect program updates or virus scan tasks.

Exit – close Kaspersky Anti-Virus for Windows Workstations (when this option is selected, the application will be unloaded from the computer's RAM).

If a virus search task is running, the context menu will display its name with a percentage progress meter. By selecting the task, you can open the report window to view current performance results.

4.3. Main program window

The Kaspersky Anti-Virus for Windows Workstations main window (see Figure 2) can be logically divided into two parts:

- the left part of the window, the navigation panel, guides you quickly and easily to any component, virus scan and update task performance, or the program's support tools;
- the right part of the window, the information panel, contains information on the protection component selected in the left part of the window and displays settings for each of them, giving you tools to carry out virus scans, work with quarantined files and backup copies, manage license keys, and so on.

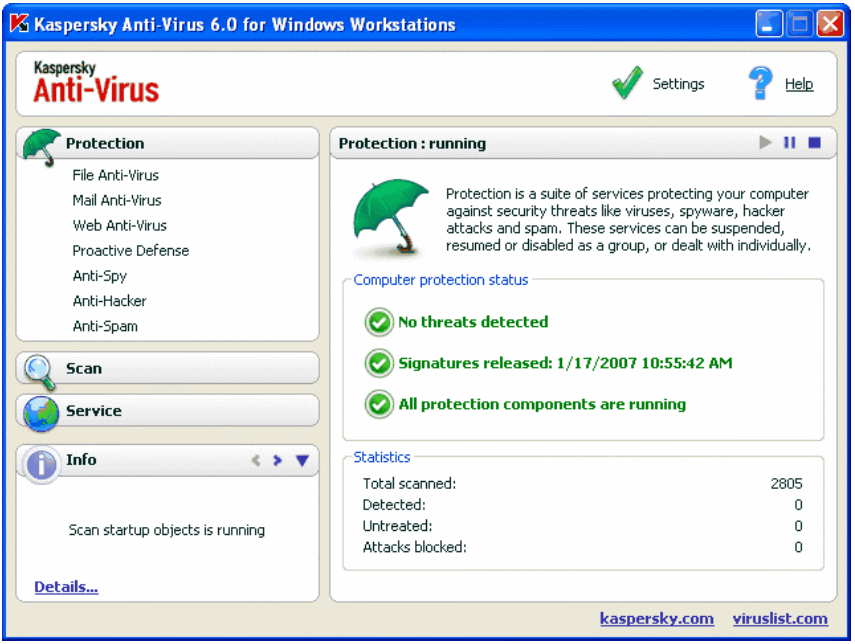
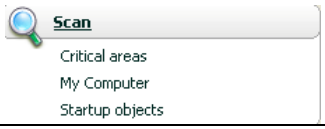
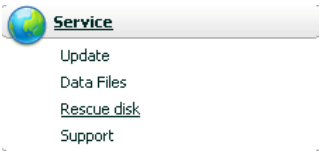
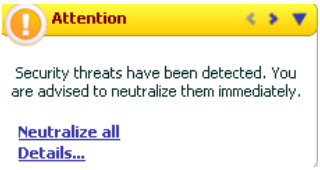


Figure 2. Kaspersky Anti-Virus for Windows Workstations main window

After selecting a section or component in the left part of the window, you will find information in the right-hand part that matches your selection.

We will now examine the elements in the main window's navigation panel in greater detail.

Main Window Section	Purpose
This window mostly informs you of the protection status of your computer. The **Protection** section is designed for exactly that. 	To see general information on operation of Kaspersky Anti-Virus, review overall statistics for program operation, and make sure that all components are working correctly, select the **Protection** section in the navigation area. You can also enable/disable protection components here. To view statistics and settings for a specific protection component, you need only select the name of the component about which you want information in the **Protection** section.
To scan your computer for malicious files or programs, use the special **Scan** section in the main window. 	This section contains a list of objects that can be scanned for viruses. The commonest and most important tasks are included in the section. These include virus scan tasks for critical areas, for startup programs, and a full computer scan.
The **Service** section includes additional Kaspersky Anti-Virus for Windows Workstations features. 	Here you can update the program, view reports on the performance of any of the Kaspersky Anti-Virus for Windows Workstations components or tasks, work with quarantined objects and backup copies, review technical support information, create a Rescue Disk and manage license keys.

Main Window Section	Purpose
The **Comments and tips** section accompanies you as you use the application. 	This section offers tips on raising the security level of your computer. You will also find comments on the application's current performance and its settings. The links in this section guide you to take the actions recommended for a particular section or to view information in more detail.

Each element of the navigation panel is accompanied by a special context menu. The menu contains points for the protection components and tools that help the user quickly configure them, manage them, and view reports. There is an additional menu item for virus scan and update tasks that allows you to create your own task, by modifying a copy of an existing task.

You can change the appearance of the program by creating and using your own graphics and color schemes.

4.4. Program settings window

You can open the Kaspersky Anti-Virus for Windows Workstations settings window from the main window (see 4.3 on pg. 50). To do so, click Settings in the upper part of it.

The settings window (see Figure 3) is similar in layout to the main window:

- the left part of the window gives you quick and easy access to the settings for each of the program components, update and virus scan tasks, and program tools;
- the right part of the window contains a detailed list of settings for the item selected in the left part of the window.

When you select any section, component, or task in the left part of the settings window, the right part will display its basic settings. To configure advanced settings, you can open second and third level settings windows. You can find a detailed description of program settings in the appropriate sections hereof.

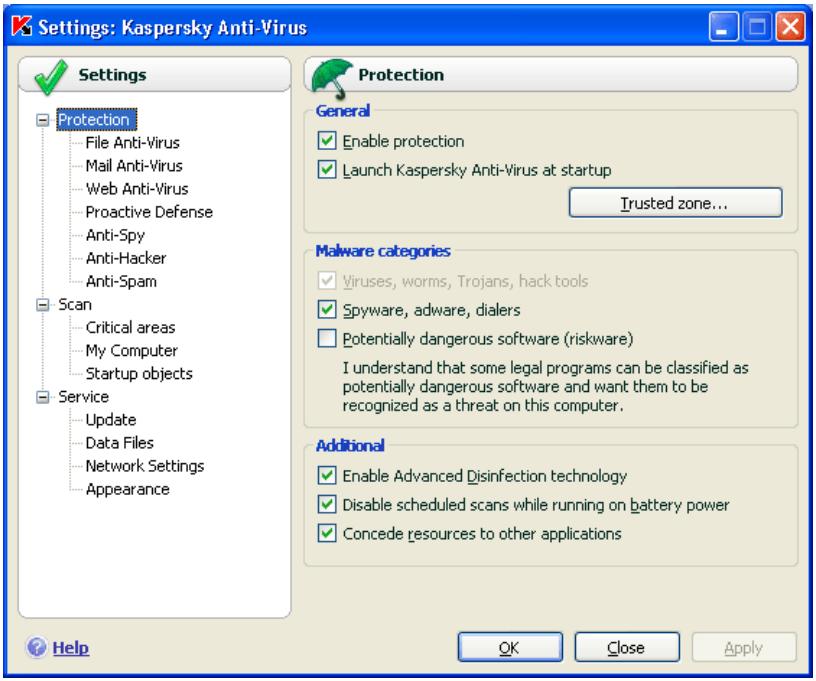


Figure 3. Kaspersky Anti-Virus for Windows Workstations settings window

CHAPTER 5. GETTING STARTED

One of Kaspersky Lab's main goals in creating Kaspersky Anti-Virus for Windows Workstations was to provide optimum configuration for each of the program's options. This makes it possible for a user with any level of computer literacy to quickly protect their computer straight after installation.

However, configuration details for your computer, or the jobs you use it for, can have their own specific requirements. That is why we recommend performing a preliminary configuration to achieve the most flexible, personalized protection of your computer.

To make getting started easier, we have combined all the preliminary configuration stages in one Setup Wizard (see 3.2 on pg. 36) that starts as soon as the program is installed. By following the Wizard's instructions, you can activate the program, configure settings for updates and virus scans, password-protect access to the program, and configure Anti-Hacker to match your network's properties.

After installing and starting the program, we recommend that you take the following steps:

- Check the current protection status (see 5.1 on pg. 55) to make sure that Kaspersky Anti-Virus for Windows Workstations is running at the appropriate level.
- Train Anti-Spam (see 5.5 on pg. 63) using your emails.
- Update the program (see 5.6 on pg. 64) if the Settings Wizard did not do so automatically after installing the program.
- Scan the computer (see 5.2 on pg. 61) for viruses.

5.1. What is the protection status of the computer?

Composite information on your computer's protection is provided in the main program window, in the **Protection** section. The *current protection status* of the computer and the *general performance statistics* of the program are displayed here.

Protection status displays the current state of protection for your computer using special indicators (see 5.1.1 on pg. 56). Statistics (see 5.1.2 on pg. 59) analyses the current program session.

5.1.1. Protection indicators

Protection status is determined by three indicators, each of which reflect a different aspect of your computer's protection at any given moment, and indicate any problems in program settings and performance.

Figure 4. Indicators reflecting the computer protection status

Each indicator has three possible appearances:

– *the situation is normal*; the indicator is showing that your computer's protection is adequate, and that there are no problems in the program settings or performance.

– *there are one or more deviations* in Kaspersky Anti-Virus for Windows Workstations performance from the recommended level of performance, which could affect information security. Please pay heed to the actions recommended by Kaspersky Lab, which are given as links.

– *the computer's security status is critical*. Please follow the recommendations closely to improve your computer's protection. The recommended actions are given as links.

We will now examine protection indicators and the situations that each of them indicate in more detail.

The first indicator reflects the situation with malicious files and programs on your computer. The three values of this indicator mean the following:

	No threats detected Kaspersky Anti-Virus for Windows Workstations has not detected any dangerous files or programs on your computer.

	All threats have been neutralized Kaspersky Anti-Virus for Windows Workstations has treated all infected files and programs, and deleted those that could not be treated.
	Threats have been detected Your computer is at risk of infection. Kaspersky Anti-Virus for Windows Workstations has detected malicious programs (viruses, Trojans, worms, etc.) that must be neutralized. To do so, use the Neutralize all link. Click the Details link to see more detailed information about the malicious objects.

The second indicator shows the effectiveness of your computer's protection. The indicator takes one of the following values:

	Signatures released: (date, time) Both the application and the threat signatures used by Kaspersky Anti-Virus for Windows Workstations are most recent versions.
	Signatures are out of date The program modules and Kaspersky Anti-Virus for Windows Workstations threat signatures have not been updated for several days. You are running the risk of infecting your computer with new malicious programs that have appeared since you last updated the program. We recommend updating Kaspersky Anti-Virus for Windows Workstations. To do so, use the Update link.
	Signatures are partially corrupted The threat signature files are partially corrupted. If this occurs, it is recommended to run program updates again. If you encounter the same error message again, contact the Kaspersky Lab Technical Support Service.
	Please restart your computer You must restart your system for the program to run correctly. Save and close all files that you are working with and use the Restart computer link.

	Program updates are disabled The threat signature and program module update service is disabled. To maintain real-time protection, we recommend enabling updates.
	Signatures are obsolete Kaspersky Anti-Virus for Windows Workstations has not been updated for some time. You are putting the data at great risk. Update the program as soon as possible. To do so, use the Update link.
	Signatures are corrupted The threat signature files are fully corrupted. If this occurs, it is recommended to run program updates again. If you encounter the same error message again, contact the Kaspersky Lab Technical Support Service.

The third indicator shows the current functionality of the program. The indicator takes one of the following values:

	All protection components are running Kaspersky Anti-Virus for Windows Workstations is protecting your computer on all channels by which malicious programs could penetrate. All protective components are enabled.
	Protection is not installed When Kaspersky Anti-Virus for Windows Workstations was installed, none of the monitoring components were installed. This means you can only scan for viruses. For maximum security, you should install protection components on your computer.
	All protection components are paused All protection components have been paused. To restore the components, select **Resume protection** from the context menu by clicking on the system tray icon.

	Some protection components are disabled One or several protection components is stopped. This could lead to your computer becoming infected and losing data. You are strongly advised to enable protection. To do so, select an inactive component from the list and click ▶.
	All protection components are disabled Protection is fully disabled. No components are running. To restore the components, select **Resume protection** from the context menu by clicking on the system tray icon.
	Some protection components have malfunctioned One or more Kaspersky Anti-Virus for Windows Workstations components has internal errors. If this occurs, you are advised to enable the component or restart the computer, as it is possible that the component drivers have to be registered after being updated.

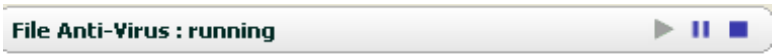
5.1.2. Kaspersky Anti-Virus for Windows Workstations component status

To determine how Kaspersky Anti-Virus for Windows Workstations is guarding your file system, email, HTTP traffic, or other areas where dangerous programs could penetrate your computer, or to view the progress of a virus scan task or threat signature update, simply open the corresponding section of the main program window.

For example, to view the current File Anti-Virus status, select **File Anti-Virus** from the left-hand panel of the main window, or to see if you are being protected against new viruses, select **Proactive Defense**. The right-hand panel will display a summary of information about the component's operation.

For protection components, the right-hand panel contains the **status bar**, the **Status** box and the **Statistics** box.

For the File Anti-Virus component, the *status bar* appears as follows:



- *File Anti-Virus : running* – file protection is active for the level selected (see 7.1 on pg. 87).

- *File Anti-Virus : paused* – File Anti-Virus is disabled for a set period of time. The component will resume operation automatically after the assigned period has expired or after the program is restarted. You can also resume file protection manually, by clicking the ▶ button located on the status bar.
- *File Anti-Virus : stopped* – the component has been stopped by the user. You can resume file protection manually, by clicking the ▶ button located on the status bar.
- *File Anti-Virus : not running* – file protection is not available for some reason.
- *File Anti-Virus : disabled (error)* – the component encountered an error.

  If a component encounters an error, try restarting it. If restart should result in an error, review component report which might contain the reason for the failure. If you are unable to troubleshoot the issue on your own, save the component report to a file using **Action → Save As** and contact Kaspersky Lab Technical Support.

If the component contains several modules, the **Status** section will contain information on the status of each of them. For components that do not have individual modules, their status, security level, and, for some components, the response to dangerous programs are displayed.

There is no **Status** box for virus scan and update tasks. The security level, the action applied to dangerous programs for virus scan tasks, and the run mode for updates are listed in the **Settings** box.

The **Statistics** box contains information on the operation of protection components, updates, or virus scan tasks.

5.1.3. Program performance statistics

Program statistics can be found in the **Statistics** box of the main window's **Protection** section, and display general information on computer protection, recorded from the time that Kaspersky Anti-Virus for Windows Workstations was installed.

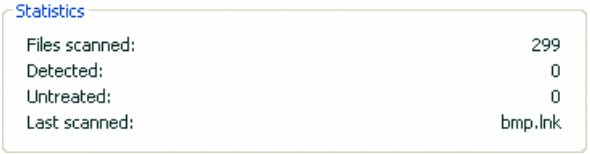


Figure 5. The program's general statistics box

You can left-click anywhere in the box to view a report with detailed information. The tabs display:

- Information on objects found (see 17.3.2 on pg. 227) and the status assigned to them
- Event log (see 17.3.3 on pg. 228)
- General scan statistics (see 17.3.4 on pg. 229) for your computer
- Program performance settings (see 17.3.5 on pg. 230)

5.2. How to scan your computer for viruses

After installation, the application will without fail inform you with a special notice in the lower left-hand part of the application window that the computer has not yet been scanned and will recommend that you scan it for viruses immediately.

Kaspersky Anti-Virus for Windows Workstations includes a task for a computer virus scan located in the **Scan** section of the program's main window.

After selecting the task **Critical Areas** you will be able to view statistics for the most recent computer scan and task settings: statistics for the most recent scan of these areas; task settings; what level of protection was selected, and what actions are applied to security threats. Here you can also select which critical areas you want to scan, and immediately scan those areas.

To scan critical areas of your computer for malicious programs,

1. Open main program window and select the task **Critical Areas** in the **Scan** section.
2. Click the **Scan** button.

Click the **Scan** button. As a result, the program will start scanning your computer, and the details will be shown in a special window. When you click the **Close** button, the progress window will be hidden, but the scan will not stop.

5.3. How to scan critical areas of the computer

There are areas on your computer that are critical from a security perspective. These are targeted by malicious programs which aim to damage your computer's hardware, including operating system, processor, memory, etc.

It is extremely important to protect these critical areas so that your computer keeps running. There is a special virus scan task for these areas, which is located in the program's main window in the **Scan** section.

After selecting the task named **Critical Areas**, the right-hand panel of the main window will display the following: statistics for the most recent scan of these areas; task settings; what level of protection was selected, and what actions are applied to security threats. Here you can also select which critical areas you want to scan, and immediately scan those areas.

To scan critical areas of your computer for malicious programs,

1. Open main program window and select the task **Critical Areas** in the **Scan** section.
2. Click the **Scan** button.

When you do this, a scan of the selected areas will begin, and the details will be shown in a special window. When you click the **Close** button, the progress window will be hidden, but the scan will not stop.

5.4. How to scan a file, folder or disk for viruses

There are situations when it is necessary to scan individual objects for viruses but not the entire computer. For example, one of the hard drives, on which your programs and games, e-mail databases brought home from work, and archived files that came with e-mail are located, etc. You can select an object for scan with the standard tools of the Microsoft Windows operating system (for example, in the **Explorer** program window or on your **Desktop**, etc.).

To scan an object,

Place the cursor over the name of the selected object, open the Windows context menu by right-clicking, and select **Scan for viruses** (see Figure 6).

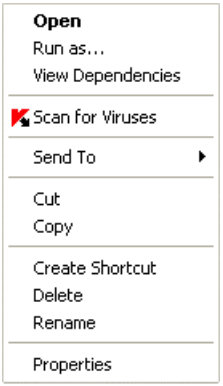


Figure 6. Scanning an object selected using a standard Windows context-sensitive menu

A scan of the selected object will then begin, and the details will be shown in a special window. When you click the **Close** button, the progress window will be hidden, but the scan will not stop.

5.5. How to train Anti-Spam

One step in getting started is training Anti-Spam to work with your emails and filter out junk. Spam is junk email, although it is difficult to say what constitutes spam for a given user. While there are email categories which can be applied to spam with a high degree of accuracy and generality (for example, mass emailings, advertisements), such emails could belong in the inbox of some users.

Therefore, we ask that you determine for yourself what email is spam and what isn't. Kaspersky Anti-Virus for Windows Workstations will ask you after installation if you want to train Anti-Spam to differentiate between spam and accepted email. You can do this with special buttons that plug into your email client (Microsoft Outlook, Outlook Express (Windows Mail), The Bat!) or using the special training wizard.

Warning!

This version of Kaspersky Anti-Virus does not provide Anti-Spam plug-ins for Microsoft Office Outlook running under Microsoft Windows 98.

To train Anti-Spam using the plug-in's buttons in the email client,

1. Open your computer's default email client (e.g. Microsoft Office Outlook). You will see two buttons on the toolbar: **Spam** and **Not Spam**.

2. Select an accepted email or group of emails that contains accepted email and click **Not Spam**. From this point onward, emails from the addresses in the emails from the senders you selected will never be processed as spam.

3. Select an email, a group of emails, or a folder of emails that you consider spam, and click **Spam**. Anti-Spam will analyze the contents of these emails, and in the future it will consider all emails with similar contents to be spam.

To train Anti-Spam using the Training Wizard,

1. Open the application settings window, select the Anti-Spam component under **Protection** and click **Training Wizard**.

2. Follow instructions displayed by the Anti-Spam Training Wizard (see 13.2.1, pg. 167).

When an email arrives in your inbox, Anti-Spam will scan it for spam content and add a special [Spam] tag to the subject line of spam. You can configure a special rule in your email client for these emails, such as a rule that deletes them or moves them to a special folder.

5.6. How to update the program

Kaspersky Lab updates the threats signatures and modules for Kaspersky Anti-Virus for Windows Workstations using dedicated update servers.

Kaspersky Lab's update servers are the Kaspersky Lab Internet sites where the program updates are stored.

Warning!

You will need a connection to the Internet to update Kaspersky Anti-Virus for Windows Workstations.

By default, Kaspersky Anti-Virus for Windows Workstations automatically checks for updates on the Kaspersky Lab servers. If the server has the latest updates, Kaspersky Anti-Virus for Windows Workstations will download and install them in the silent mode.

To update Kaspersky Anti-Virus for Windows Workstations manually,

select the **Update** component in the **Service** section of the main program window and click the **Update now!** button in the right-hand part of the window.

As a result, Kaspersky Anti-Virus for Windows Workstations will begin the update process, and display the details of the process in a special window.

5.7. What to do if protection is not running

If problems or errors arise in the performance of any protection component, be sure to check its status. If the component status is *not running* or *disabled (operation error)*, try restarting Kaspersky Anti-Virus.

If the problem is not solved by restarting the program, we recommend fixing potential errors using the program restore feature (see Chapter 19, pg. 279).

If the restore procedure does not help, contact Kaspersky Lab Technical Support. You may need to save a report on component operation or for the entire application to file and send it to Technical Support for investigation.

To save the report to file:

1. Select the component in the **Protection** section of the main window of the program and left-click anywhere in the **Statistics** box.
2. Click the **Save As** button and in the window that opens specify the file name for the component's performance report.

To save a report for all Kaspersky Anti-Virus for Windows Workstations components at once (protection components, virus scan tasks, support features):

1. Select the **Protection** section in the main window of the program and left-click anywhere in the **Statistics** box.

   or

   Click All reports in the report window for any component. Then the **Reports** tab will list reports for all program components.
2. Click the **Save As** button and in the window that opens specify a file name for the program's performance report.

CHAPTER 6. PROTECTION MANAGEMENT SYSTEM

Kaspersky Anti-Virus for Windows Workstations lets you multi-task computer security management:

- Enable, disable, and pause (see 6.1 on pg. 66) the program
- Define the types of dangerous programs (see 6.2 on pg. 70) against which Kaspersky Anti-Virus for Windows Workstations will protect your computer
- Create an exclusion list (see 6.3 on pg. 71) for protection
- Create your own virus scan and update tasks (see 6.4 on pg. 81).
- Configure a virus scan schedule (see 6.5 on pg. 82).
- Configure productivity settings (see 6.6 on pg. 84) for antivirus protection

6.1. Stopping and resuming protection on your computer

By default, Kaspersky Anti-Virus boots at startup and protects your computer the entire time you are using it. The words *Kaspersky Anti-Virus 6.0* in the upper right-hand corner of the screen let you know this. All protection components (see 2.2.1 on pg. 24) are running.

You can fully or partially disable the protection provided by Kaspersky Anti-Virus for Windows Workstations.

Warning!

Kaspersky Lab strongly recommend that you **do not disable protection**, since this could lead to an infection on your computer and consequent data loss.

Note that in this case protection is discussed in the context of the protection components. Disabling or pausing protection components does not affect the performance of virus scan tasks or program updates.

6.1.1. Pausing protection

Pausing protection means temporarily disabling all the components that monitor the files on your computer, incoming and outgoing email, executable scripts, application behavior, and Anti-Hacker and Anti-Spam.

To pause a Kaspersky Anti-Virus for Windows Workstations operation:

1. Select **Pause protection** in the program's context menu (see 4.2 on pg. 49).
2. In the Pause Protection window that opens (see Figure 7), select how soon you want protection to resume:
   - **In <time interval>** – protection will resume this far in the future. Use the dropdown menu to select the time interval.
   - **At next program restart** – protection will resume if you open the program from the Start Menu or after you restart your computer (provided the program is set to start automatically when you turn on your computer (see 6.1.5 on pg. 70)).
   - **By user request only** – protection will stop until you start it yourself. To enable protection, select **Resume protection** from the program's context menu.

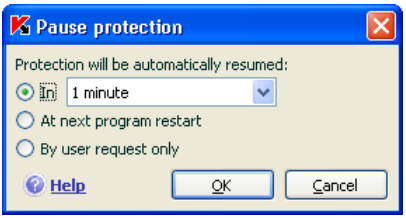


Figure 7. Pause protection window

> Tip:
>
> You can also stop protection on your computer with one of the following methods:
>
> - Click the ❚❚ button in the **Protection** section.
> - Select **Exit** from the context menu. In this case the program will be unloaded from the computer's memory.

If you pause protection, all protection components will be paused. This is indicated by:

- Inactive (gray) names of the disabled components in the **Protection** section of the main window.
- Inactive (gray) system tray icon.
- The third protection indicator (see 5.1.1 on pg. 56) on your computer, which shows that **All protection components are paused**.

6.1.2. Stopping protection

Stopping protection means fully disabling your components. Virus scans and updates continue to work in this mode.

If protection is stopped, it can be only be resumed by the user: protection components will not automatically resume after system or program restarts. Remember that if Kaspersky Anti-Virus for Windows Workstations is somehow in conflict with other programs installed on your computer, you can pause individual components or create an exclusion (see 6.3 on pg. 71) list.

To stop all protection:

1. Open the Kaspersky Anti-Virus settings window and select **Protection**.
2. Uncheck **Enable protection**.

After disabling protection, all protection components will stop. This is indicated by:

- Inactive (gray) names of the disabled components in the Protection section of the main window.
- Inactive (gray) system tray icon.
- The third protection indicator (see 5.1.1 on pg. 56) on your computer, which shows that **All protection components are disabled**.

6.1.3. Pausing / stopping protection components and tasks

There are several ways to stop a protection component, virus scan, or update. Before doing so, you are strongly advised to establish why you need to stop them. It is likely that the problem can be solved in another way, for example, by changing the security level. If, for example, you are working with a database that you are sure does not contain viruses, simply add its files as an exclusion (see 6.3 on pg. 71).

To pause protection components, virus scans, and update tasks:

Select the component or task from the left-hand part of the main window and click the button on the status bar.

The component/task status will change to ***paused***. The component or task will be paused until you resume it by clicking the button.

When you pause a component or task, Kaspersky Anti-Virus statistics for the current Kaspersky Anti-Virus for Windows Workstations session are saved and will continue to be recorded after the component or task is updated.

To stop protection components, virus scans, and update tasks:

Click the button on the status bar. You can also stop protection components in the program settings window by deselecting **Enable <component name>** in the **General** section for that component.

The component/task status will then change to *stopped (disabled)*. The component or task will be stopped until you enable it by clicking the button. For virus scan and update tasks, you will have the choice of the following options: continue the task that was interrupted, or restart it from the beginning.

When you stop a component or task, all the statistics from previous work are cleared and when the component is started they are recorded over.

6.1.4. Restoring protection on your computer

If at some point you paused or stopped protection on your computer, you can resume it using one of the following methods:

- *From the context menu*.

  To do so, select **Resume protection**.

- *From the program's main window*.

  To do so, click the button on the status bar in the **Protection** section of the main window.

The protection status immediately changes to ***running***. The program's system tray icon becomes active (color). The third protection indicator (see 5.1.1 on pg. 56) will also inform you that **All protection components are enabled**.

6.1.5. Shutting down the program

If you have to shut down Kaspersky Anti-Virus for Windows Workstations, select **Exit** from the program's context menu (see 4.2 on pg. 49). This will close the program, leaving your computer unprotected.

If network connections that the program monitors are active on your computer when you close the program, a notice will appear on the screen stating that these connections will be interrupted. This is necessary for the program to shut down correctly. The connections are terminated automatically after ten seconds or by clicking the **Yes** button. The majority of connections will resume after a brief time.

Note that if you are downloading a file without a download manager when the connection is terminated, the file transfer will be lost. You will have to download the file over again.

You can choose not to interrupt the connections by clicking on the **No** button in the notice window. If you do so, the program will continue running.

After closing the program, you can enable computer protection again by opening Kaspersky Anti-Virus for Windows Workstations (**Start→ Programs → Kaspersky Anti-Virus 6.0 for Windows Workstations → Kaspersky Anti-Virus 6.0 for Windows Workstations**).

You can also resume protection automatically after restarting your operating system. To enable this feature, select the **Protection** section in the program settings window and check **Launch Kaspersky Anti-Virus at startup**.

6.2. Types of malicious programs to be monitored

Kaspersky Anti-Virus for Windows Workstations protects you from various types of malicious programs. Current settings notwithstanding, the application will always secure your computer against the most dangerous types of malicious software, such as viruses, Trojans, and hack tools. These programs can do significant damage to your computer. To make your computer more secure, you can expand the list of threats that the program will detect by making it monitor additional types of dangerous programs.

To choose what malicious programs Kaspersky Anti-Virus for Windows Workstations will protect you from, select the **Protection** section in the program settings window (see 4.4 on pg. 53).

The **Malware categories** box contains threat types (see 1.1on pg. 11):

- **Viruses, worms, Trojans, hack tools**. This group combines the most common and dangerous categories of malicious programs. This is the minimum admissible security level. Per recommendations of Kaspersky Lab experts, Kaspersky Anti-Virus always monitors this category of malicious programs.
- **Spyware, adware, dialers**. This group includes potentially dangerous software that may inconvenience the user or incur serious damage.
- **Potentially dangerous software (riskware)**. This group includes programs that are not malicious or dangerous. However, under certain circumstances they could be used to cause harm to your computer.

The groups listed above comprise the full range of threats which the program detects when scanning objects.

If all groups are selected, Kaspersky Anti-Virus for Windows Workstations provides the fullest possible anti-virus protection for your computer. If the second and third groups are disabled, the program will only protect you from the commonest malicious programs. This does not include potentially dangerous programs and others that could be installed on your computer and could damage your files, steal your money, or take up your time.

Kaspersky Lab does not recommend disabling monitoring for the second group. When situations arise when Kaspersky Anti-Virus for Windows Workstations classifies a program as potentially dangerous that you feel is not, we recommend configure an exclusion for it (see 6.3 on pg. 71).

6.3. Creating a trusted zone

A *trusted zone* is a list of objects created by the user, that Kaspersky Anti-Virus for Windows Workstations does not monitor. In other words, it is a set of programs excluded from protection.

The user creates a protected zone based on the properties of the files he uses and the programs installed on his computer. You might need to create such an exclusion list if, for example, Kaspersky Anti-Virus for Windows Workstations blocks access to an object or program and you are sure that the file or program is absolutely safe.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects according to the status that the program assigns to objects during a scan.

Warning!

An exclusion object is not scanned when the disk or folder where it is located is scanned. However, if you select that object specifically, the exclusion rule will not be applied.

In order to create an exclusion list,

1. Open the application settings window and select the **Protection** section.
2. Click the **Trusted Zone** button in the **General** section.
3. Configure exclusion rules for objects and create a list of trusted applications in the window that opens (see Figure 8).

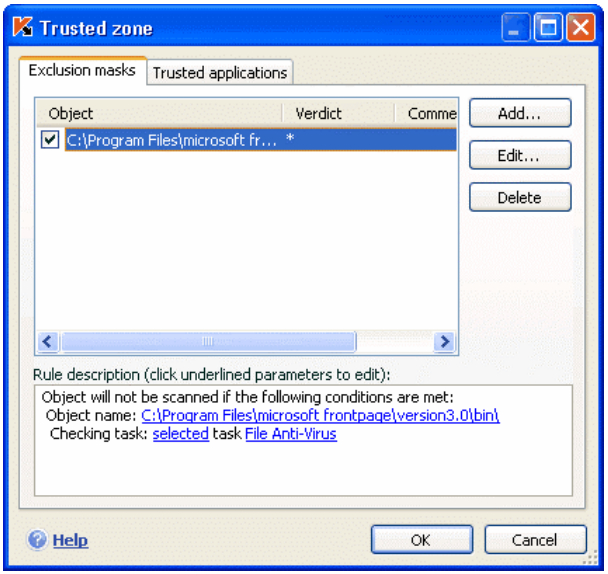


Figure 8. Creating a trusted zone

6.3.1. Exclusion rules

Exclusion rules are sets of conditions that Kaspersky Anti-Virus for Windows Workstations uses to determine not to scan an object.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area, such as a folder or a program, program processes, or objects according to their verdict.

The *verdict* is the status that Kaspersky Anti-Virus for Windows Workstations assigns to an object during the scan. A verdict is based on the classification of malicious and potentially dangerous programs found in the Kaspersky Lab Virus Encyclopedia.

Potentially dangerous software does not have a malicious function but can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration programs, IRC clients, FTP servers, all-purpose utilities for stopping or hiding processes, keyloggers, password macros, autodialers, etc. These programs are not classified as viruses. They can be divided into several types, e.g. Adware, Jokes, Riskware, etc. (for more information on potentially dangerous programs detected by Kaspersky Anti-Virus for Windows Workstations, see the Virus Encyclopedia at www.viruslist.com). After the scan, these programs may be blocked. Since several of them are very common, you have the option of excluding them from the scan. To do so, you must specify the verdict assigned to that program as an exclusion mask.

For example, imagine you use a Remote Administrator program frequently in your work. This is a remote access system with which you can work from a remote computer. Kaspersky Anti-Virus for Windows Workstations views this sort of application activity as potentially dangerous and may block it. To keep the application from being blocked, you must create an exclusion rule that specifies *not-a-virus:RemoteAdmin.Win32.RAdmin.22* as the verdict.

When you add an exclusion, a rule is created that several program components (File Anti-Virus, Mail Anti-Virus, Web Anti-Virus, Proactive Defense) and virus scan tasks can later use. You can create exclusion rules in a special window that you can open from the program settings window, from the notice about detecting the object, and from the report window.

*To add exclusions on the **Exclusion Rule** tab:*

1. Click on the **Add** button in the **Exclusion mask** tab.
2. In the window that opens (see Figure 9), click the exclusion type in the **Properties** section:

- **Object** – exclusion of a certain object, directory, or files that match a certain mask from scans.
- **Verdict** – excluding an object from the scan based on its status from the Virus Encyclopedia classification.

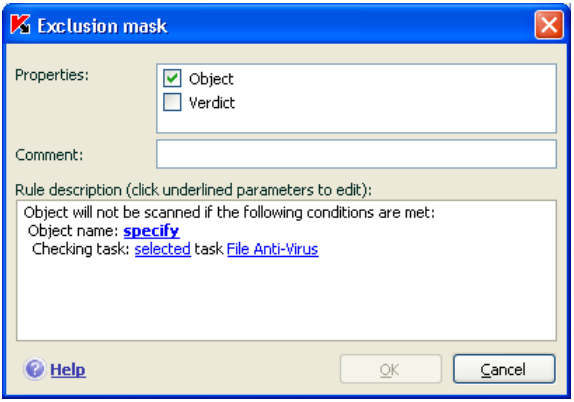


Figure 9. Creating an exclusion rule

If you check both boxes at once, a rule will be created for that object with a certain status according to Virus Encyclopedia classification. In such a case, the following rules apply:

- If you specify a certain file as the **Object** and a certain status in the **Verdict** section, the file specified will only be excluded if it is classified as the threat selected during the scan.
- If you select an area or folder as the **Object** and the status (or verdict mask) as the **Verdict**, then objects with that status will only be excluded when that area or folder is scanned.

3. Assign values to the selected exclusion types. To do so, left-click in the **Rule description** section on the specify link located next to the exclusion type:

   - For the **Object** type, enter its name in the window that opens (this can be a file, a particular folder, or a file mask (see A.2 on pg. 305). Check **Include subfolders** for the object (file, file mask, folder) to be recursively excluded from the scan. For example, if you assign **C:\Program Files\winword.exe** as an exclusion and checked the scan nested folders option, the file **winword.exe** will be excluded from the scan if found in any folder under **C:\Program Files**.
   - Enter the full name of the threat that you want to exclude from scans as given in the Virus Encyclopedia or use a mask (see A.3 on pg. 305) for the **Verdict**.

     For some verdicts, you can assign advanced conditions for applying rules in the **Advanced settings** field (see A.3 on

pg. 305). In most cases, this field is filled in automatically when you add an exclusion rule from a Proactive Defense notification.

You can add advanced settings for the following verdicts, among others:

- *Invader*. For this verdict, you can give a name, mask, or complete path to the object being embed (for example, a .dll file) as an additional exclusion condition.
- *Launching Internet Browser*. For this verdict, you can list browser open settings as additional exclusion settings.
  For example, you blocked browsers from opening with certain settings in the Proactive Defense application activity analysis. However, you want to allow the browser to open for the domain *www.kasperky.com* with a link from Microsoft Office Outlook as an exclusion rule. To do so, select Microsoft Office Outlook as the exclusion **Object** and *Launching Internet Browser* as the **Verdict**, and enter an allowed domain mask in the **Advanced settings** field.

4. Define which Kaspersky Anti-Virus for Windows Workstations components will use this rule. If item any is selected, this rule will apply to all components. If you want to restrict the rule to one or several components, click on any, which will change to selected. In the window that opens, check the boxes for the components that you want this exclusion rule to apply to.

To create an exclusion rule from a program notice stating that it has detected a dangerous object:

1. Use the Add to trusted zone link in the notification window (see Figure 10).
2. In the window that opens, be sure that all the exclusion rule settings match your needs. The program will fill in the object name and threat type automatically, based on information from the notification. To create the rule, click **OK**.

Figure 10. Dangerous object detection notification

To create an exclusion rule from the report window:

1. Select the object in the report that you want to add to the exclusions.
2. Open the context menu and select **Add to Trusted zone** (see Figure 11).

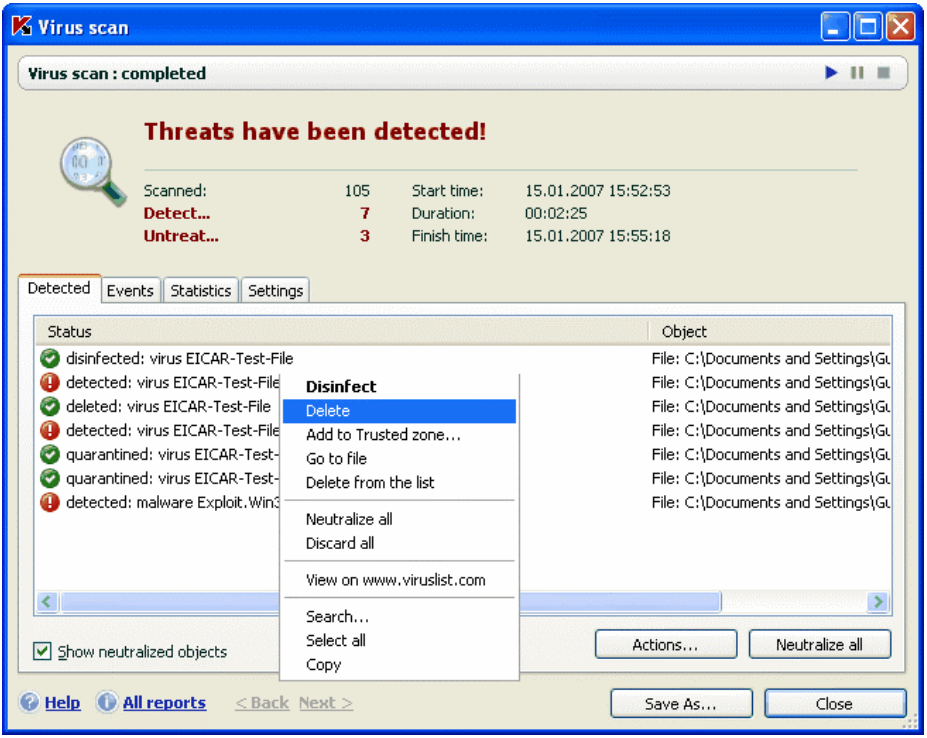


Figure 11. Creating an exclusion rule from a report

3. The exclusion settings window will then open. Be sure that all the exclusion rule settings match your needs. The program will fill in the object name and threat type automatically based on the information from the report. To create the rule, click **OK**.

6.3.2. Trusted applications

You can only exclude trusted applications from the scan in Kaspersky Anti-Virus if installed on a computer running Microsoft Windows NT 4.0/2000/XP/Vista.

Kaspersky Anti-Virus provides the capability to create a list of trusted applications whose activity, suspicious or otherwise, and file, network, and system registry access, are not monitored.

For example, you feel that objects and processes used by Windows **Notepad** are safe and do not need to be scanned. To exclude objects used by this process

from scanning, add **Notepad** to the trusted applications list. However, the executable file and the trusted application process will be scanned for viruses as before. To fully exclude the application from scanning, you must use exclusion rules (see 6.3.1 on pg. 72).

In addition, some actions classified as dangerous are perfectly normal features for a number of programs. For example, keyboard layout toggling programs regularly intercept text entered on your keyboard. To accommodate such programs and stop monitoring their activity, you are advised to add them to the trusted application list.

Excluding trusted applications can also solve potential compatibility conflicts between Kaspersky Anti-Virus for Windows Workstations and other applications (for example, network traffic from another computer that has already been scanned by the anti-virus application) and can boost computer productivity, which is especially important when using server applications.

By default, Kaspersky Anti-Virus for Windows Workstations scans objects opened, run, or saved by any program process and monitors the activity of all programs and the network traffic they create.

You can create a list of trusted applications on the special **Trusted applications** tab (see Figure 12). By default the trusted applications list contains a list of applications that will not be monitored based on Kaspersky Lab recommendations when you install Kaspersky Anti-Virus. If you do not trust an application on the list, deselect the corresponding checkbox. You can edit the list using the **Add**, **Edit**, and **Delete** buttons on the right.

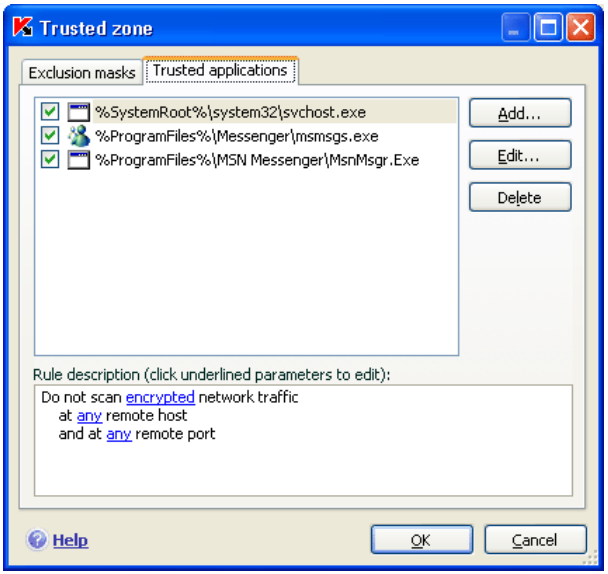


Figure 12. Trusted application list

To add a program to the trusted application list:

1. Click the **Add** button on the right-hand part of the **Trusted application** tab.
2. In the **Trusted application** window (see Figure 13) that opens, select the application using the **Browse** button. A context menu will open, and by clicking **Browse** you can go to the file selection window and select the path to the executable file, or by clicking **Applications** you can go to a list of applications currently running and select them as necessary.

When you select a program, Kaspersky Anti-Virus for Windows Workstations records the internal attributes of the executable file and uses them to identify the trusted program during scans.

The file path is inserted automatically when you select its name.

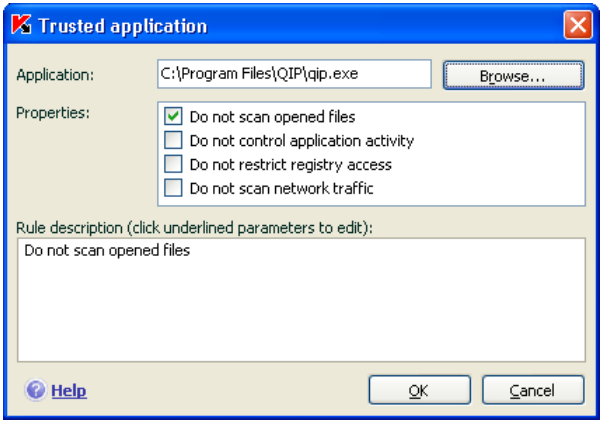


Figure 13. Adding an application to the trusted list

3. Specify which actions performed by this process will not be monitored:

   Do not scan opened files – excludes from the scan all files that the trusted application process.

   Do not restrict application activity – excludes from Proactive Defense monitoring any activity, suspicious or otherwise, that the trusted application performs.

   Do not restrict registry access – excludes from scanning any accesses of the system registry initiated by the trusted application.

   Do not scan network traffic – excludes from scans for viruses and spam any network traffic initiated by the trusted application. You can exclude all the application's network traffic or encrypted traffic (SSL) from the scan. To do so, click the all link. It will change to encrypted. In addition you can restrict the exclusion by assigning a remote host/port. To create a restriction, click any, which will change to selected, and enter a value for the remote port/host.

   Note that if **Do not scan network traffic** is checked, traffic for that application will only be scanned for viruses and spam. However, this does not affect whether Anti-Hacker scans traffic. Anti-Hacker settings govern analysis of network activity for that application.

6.4. Starting tasks under another profile

Kaspersky Anti-Virus for Windows Workstations 6.0 has a feature that can start scan tasks under another user profile. This feature is by default disabled, and tasks are run under the profile under which you are logged into the system.

The feature is useful if for example, you need access rights to a certain object during a scan. By using this feature, you can configure tasks to run under a user that has the necessary privileges.

Note that this option is not available under Microsoft Windows 98/ME.

Program updates may be made from a source to which you do not have access (for example, the network update folder) or authorized user rights for a proxy server. You can use this feature to run the Updater with another profile that has those rights.

To configure a scan task that starts under a different user profile:

1. Select the task name in the **Scan** section (for virus scans) or the Service section (for update tasks) of the main window and use the Settings link to open the task settings window.
2. Click the **Customize** button in the task settings window and go to the **Additional** tab in the window that opens (see Figure 14).

To enable this feature, check **Run this task as**. Enter the data for the login that you want to start the task as below: user name and password.

Note that if you do not run the task as a user with appropriate privileges, the scheduled update will be run with the privileges of the current user account. If no users are currently logged into the computer, running updates under another user account has not been configured, and updates run automatically, they will run with the SYSTEM privileges.

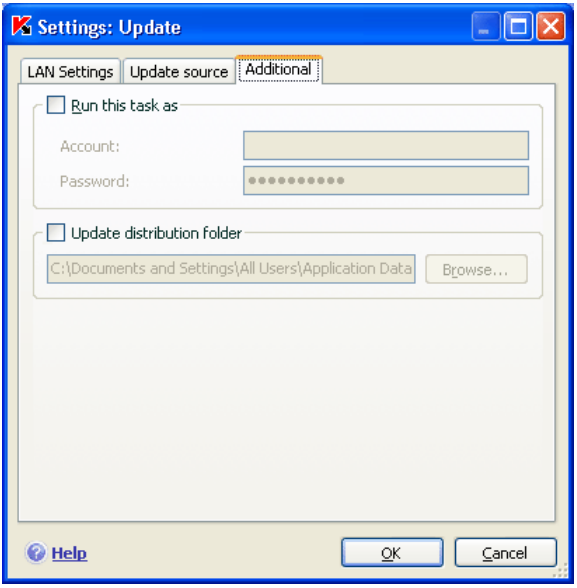


Figure 14. Configuring an update task from another profile

6.5. Configuring Scheduled Tasks and Notifications

Schedule settings are identical for virus scan tasks, application updates, and Kaspersky Anti-Virus event notifications.

By default, the virus scan tasks created at application install are disabled. Startup objects are the exception since they are scanned every time Kaspersky Anti-Virus is started. Updates are configured to occur automatically by default as updates become available on Kaspersky Lab update servers.

In the event that you are not satisfied with these settings, you may reconfigure task schedules. Select a task by name under **Virus Scan** (for virus scan tasks) or **Service** (for updates and update distribution) and open the related settings window by clicking Settings.

To have tasks start according to a schedule, check the automatic task start box in the **Run Mode** section. You can edit the times for starting the scan task in the **Schedule** window (see Figure 15), that opens when you click **Change**.

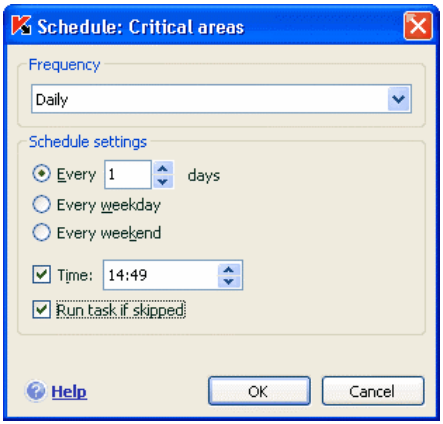


Figure 15. Configuring a task schedule

The primary setting to define is the frequency of an event (task execution or notification). Select the desired option under **Frequency** (see Figure 15). Then, settings for the selected option are to be specified under Schedule Settings. The following options are available:

- **Minutes.** The time interval between scans or notifications will be several minutes. Specify the length of time in minutes under schedule settings. It should not exceed 59 minutes.
- **Hours.** The interval between scans or notifications is several hours. If this option is selected, specify the time interval under schedule settings: **Every N hours** and specify *N*. Enter **Every 1 hour**, for instance, if you want the task to run hourly.
- **Days.** The task is started or the notification is sent at an interval of several days. Specify the interval in the schedule settings:
  - Select **Every n days** and enter a value for n if you wish to maintain an interval of several days.
  - Select **Every Weekday**, if you want the task to run daily Monday through Friday.
  - Select **Every Weekend** to run the task or send notification on Saturdays and Sundays only.

  Use the **Time** field to specify what time of day the scan task will be run.
- **Weeks.** The task is started or the notification sent on certain days of the week. If you select this option, put checkmarks next to the days of the week on which you need the task to run. Enter time of day in the **Time** field.

Months. The task is started or the notification sent once a month at a specified time.

Time. Start a task or send a notification at the specified date and time.

At Application Startup. Run task or send notification every time Kaspersky Anti-Virus starts. A time delay may also be specified relative to the start of the application for a task to be run.

After each update. The task starts after each threat signature update (this only applies to virus scan tasks).

If a task cannot run for some reason (an email program is not installed, for example, or the computer was shut down at the time), the task can be configured to run automatically as soon as it becomes possible. To do so, check **Run task if skipped** in the schedule window.

6.6. Power options

To conserve the battery of your laptop computer, and to reduce the load on the central processor and disk subsystems, you can postpone virus scans:

- Since virus scans and program updates sometimes require a fair amount of resources and can take up time, you are advised to disable schedules for these tasks, which will help you to save battery life. If necessary, you can manually update the program yourself (see 5.6 on pg. 64) or start a virus scan (see 5.2 on pg. 61). To use the battery-saving feature, check **Disable scheduled scans while running on battery power** box.
- Virus scans increase the load on the central processor and disk subsystems, thereby slowing down other programs. By default, if such a situation arises, the program pauses virus scans and frees up system resources for user applications.

  However, there are a number of programs that can be launched as soon as the processor's resources are freed and run in background mode. For virus scans not to depend on the operation of such programs, uncheck **Concede resources to other applications**.

  Note that this setting can be configured individually for every virus scan task. If you choose to do this, the configuration for a specific task has a higher priority.

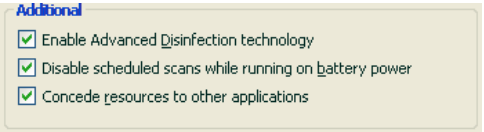

Additional
Enable Advanced Disinfection technology
Disable scheduled scans while running on battery power
Concede resources to other applications

Figure 16. Configuring power settings

To configure power settings for virus scan tasks:

Select the **Protection** section of the main program window and click Settings. Configure power settings in the **Advanced** box (see Figure 16).

6.7. Advanced Disinfection Technology

Today's malicious programs can invade the lowest levels of an operating system, which makes them practically impossible to delete. Kaspersky Anti-Virus 6.0 asks you if you want to run Advanced Disinfection Technology when it detects a threat currently active in the system. This will neutralize the threat and delete it from the computer.

After this procedure, you will need to restart your computer. After restarting your computer, we recommend running a full virus scan. To use Advanced Disinfection Technology, check **Enable Advanced Disinfection Technology**.

To enable/disable advanced disinfection technology:

Select the **Protection** section of the main program window and click the Settings link. Configure power settings in the **Additional** box (see Figure 16).

CHAPTER 7. FILE ANTI-VIRUS

The Kaspersky Anti-Virus for Windows Workstations component that protect your computer files against infection is called *File Anti-Virus.* It loads when you start your operating system, runs in your computer's RAM, and scans all files that you open, save, or execute.

The component's activity is indicated by the Kaspersky Anti-Virus for Windows Workstations system tray icon, which looks like this whenever a file is being scanned.

File Anti-Virus by default scans only *new or modified files,* that is, only files that have been added or changed since the previous scan. Files are scanned with the following algorithm:

1. Every time the user or a program accesses each time, the component intercepts it.
2. File Anti-Virus scans the iChecker™ and iSwift™ databases for information on the file intercepted. A decision is made whether to scan the file based on the information retrieved.

The scanning process includes the following steps:

1. The file is analyzed for viruses. Malicious objects are detected by comparison with the program's *threat signatures*, which contain descriptions of all malicious programs, threats, and network attacks known to date, with methods for neutralizing them.
2. After the analysis, there are three available courses of action:
    a. If malicious code is detected in the file, File Anti-Virus blocks the file, places a copy of it in *Backup*, and attempts to disinfect the file. If the file is successfully disinfected, it becomes available again. If not, the file is deleted.
    b. If code is detected in a file that appears to be malicious but there is no guarantee, the file is subject to disinfection and is sent to *Quarantine*.
    c. If no malicious code is discovered in the file, it is immediately restored.

7.1. Selecting a file security level

File Anti-Virus protects files that you are using at one of the following levels (see Figure 17):

- **High** – the level with the most comprehensive monitoring of files opened, saved, or run.
- **Recommended** – Kaspersky Lab recommends this settings level. It will scan the following object categories:
    - Programs and files by contents
    - New objects and objects modified since the last scan
    - Embedded OLE objects
- **Low** – level with settings that let you comfortably use applications that require significant system resources, since the scope of files scanned is reduced.

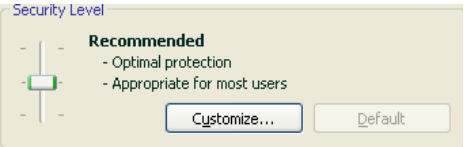


Figure 17. File Anti-Virus security level

The default setting for File Anti-Virus is **Recommended**.

You can raise or lower the protection level for files you use by either selecting the level you want, or changing the settings for the current level.

To change the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the set file security levels meet your needs, you can customize the protection settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. In such a case, the level will be set at **Custom**. Let's look at an example of when user defined file security levels could be useful.

Example:

The work you do on your computer uses a large number of file types, and some the files may be fairly large. You would not want to run the risk of

skipping any files in the scan because of the size or extension, even if this would somewhat affect the productivity of your computer.

Tip for selecting a level:

Based on the source data, one can conclude that you have a fairly high risk of being infected by a malicious program. The size and type of the files being handled is quite varied and skipping them in the scan would put your data at risk. You want to scan the files you use by contents, not by extension.

You are advised to start with the **Recommended** security level and make the following changes: remove the restriction on scanned file sizes and optimize File Anti-Virus operation by only scanning new and modified files. Then the scan will not take up as many system resources so you can comfortably use other applications.

To modify the settings for a security level:

Click the **Settings** button in the File Anti-Virus settings window. Edit the File Anti-Virus settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom**, which contains the protection settings that you configured.

7.2. Configuring File Anti-Virus

Your settings determine how File Anti-Virus will defend your computer. The settings can be broken down into the following groups:

- Settings that define what file types (see 7.2.1 on pg. 88) are to be scanned for viruses
- Settings that define the scope of protection (see 7.2.2 on pg. 91)
- Settings that define how the program responds to dangerous objects (see 7.2.5 on pg. 95)
- Additional settings for File Anti-Virus (see 7.2.3 on pg. 92)

The following sections will examine these groups in detail.

7.2.1. Defining the file types to be scanned

When you select file types to be scanned, you establish what file formats, sizes, and what drives will be scanned for viruses when opened, executed, or saved.

To make configuration easier, all files are divided into two groups: *simple* and *compound*. Simple files, for example, .txt files, do not contain any objects. Compound objects can include several objects, each of which may in turn contain other objects. There are many examples: archives, files containing macros, spreadsheets, emails with attachments, etc.

The file types scanned are defined in the **File types** section (see Figure 18). Select one of the three options:

- **Scan all files**. With this option selected, all file system objects that are opened, run, or saved will be scanned without exceptions.
- **Scan programs and documents (by contents)**. If you select this group of files, File Anti-Virus will only scan potentially infected files – files that a virus could imbed itself in.

  Note:

  There are a number of file formats that have a fairly low risk of having malicious code injected into them and subsequently being activated. An example would be .txt files.

  And vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of injection and activation of malicious code in such files is fairly high.

  Before searching for viruses in a file, its internal header is analyzed for the file format (txt, doc, exe, etc.). If the analysis shows that the file format cannot be infected, it is not scanned for viruses and is immediately returned to the user. If the file format can be infected, the file is scanned for viruses.

- **Scan programs and documents (by extension)**. If you select this option, File Anti-Virus will only scan potentially infected files, but the file format will be determined by the filename's extension. Using the extension link, you can review a list of file extensions (see A.1 on pg. 302) that are scanned with this option.

Tip:

Do not forget that someone could send a virus to your computer with an extension (e.g. .txt) that is actually an executable file renamed as a .txt file. If you select **Scan programs and documents (by extension)**, the scan would skip such a file. If **Scan programs and documents (by contents)** is selected, the extension is ignored, and analysis of the file headers will uncover that the file is an .exe file. File Anti-Virus would scan the file for viruses.

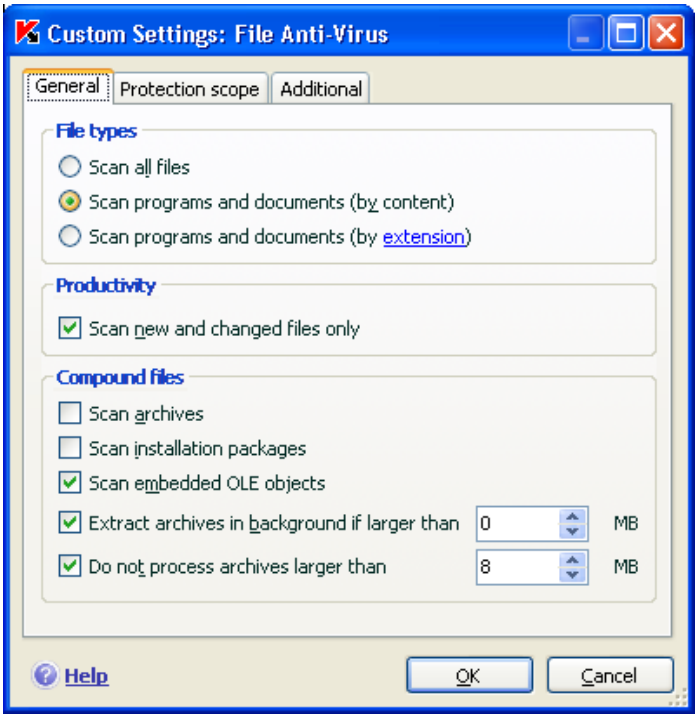


Figure 18. Selecting the file types scanned for viruses

In the **Productivity** section, you can specify that only new files and those that have been modified since the previous scan should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To select this mode, check **Scan new and changed files only**. This mode applies to both simple and compound files.

In the **Compound files** section, specify which compound files to scan for viruses:

- **Scan all/only new archives** – scans .zip, .cab, .rar, and .arj archives.
- **Scan all/only new installation packages** – scans self-extracting archives for viruses.
- **Scan all/only new embedded OLE objects** – scans objects imbedded in files (for example, Microsoft Office Excel spreadsheets or macros imbedded in a Microsoft Office Word file, email attachments, etc.).

You can select and scan all files, or only new files, for each type of compound file. To do so, left-click the link next to the name of the object to toggle its value.

If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

To specify compound files that should not be scanned for viruses, use the following settings:

- **Extract archives in background if larger than... MB**. If the size of a compound object exceeds this restriction, the program will scan it as a single object (by analyzing the header) and will return it to the user. The objects that it contains will be scanned later. If this option is not checked, access to files larger than the size indicated will be blocked until they have been scanned.
- **Do not process archives larger than... MB**. With this option checked, files larger than the size specified will be skipped by the scan.

7.2.2. Defining protection scope

By default, File Anti-Virus scans all files when they are used, regardless of where they are stored, whether it be a hard drive, CD/DVD-ROM, or flash drive.

You can limit the scope of protection. To do so:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Settings** button and select the **Protection Scope** tab (see Figure 19) in the window that opens.

The tab displays a list of objects that File Anti-Virus will scan. Protection is enabled by default for all objects on hard drives, removable media, and network drives connected to your computer. You can add to and edit the list using the **Add, Edit,** and **Delete** buttons.

If you want to protect fewer objects, you can do so using the following methods:

- Specify only folders, drives, and files that need to be protected.
- Create a list of objects that do not need to be protected (see 6.3 on pg. 71).
- Combine methods one and two – create a protection scope that excludes a number of objects.

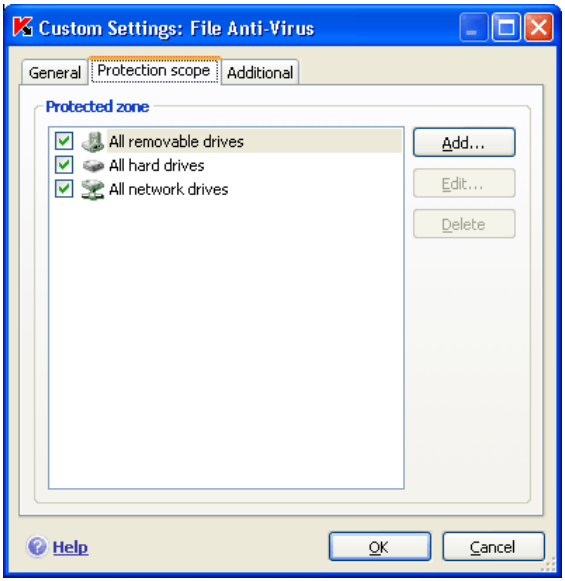


Figure 19. Defining the scope of protection

You can use masks when you add objects for scanning. Note that you can only enter masks will absolute paths to objects:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** - all files in folder *C:\dir*
- **C:\dir*.exe** - all files with the extension .exe in the folder *C:\dir*
- **C:\dir*.ex?** – all files with the extension .ex? in the folder *C:\dir*, where ? can represent any one character
- **C:\dir\test** – only the file C:\dir\test

In order for the scan to be carried out recursively, check **Include subfolders**.

Warning!

Remember that File Anti-Virus will scan only the files that are included in the protection scope created. Files not included in that scope will be available for use without being scanned. This increases the risk of infection on your computer.

7.2.3. Configuring advanced settings

As additional File Anti-Virus settings, you can specify the file system scanning mode and configure the conditions for temporarily pausing the component.

To configure additional File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking the Settings link.
2. Click the **Customize** button and select the **Additional** tab in the window that opens (see Figure 20).

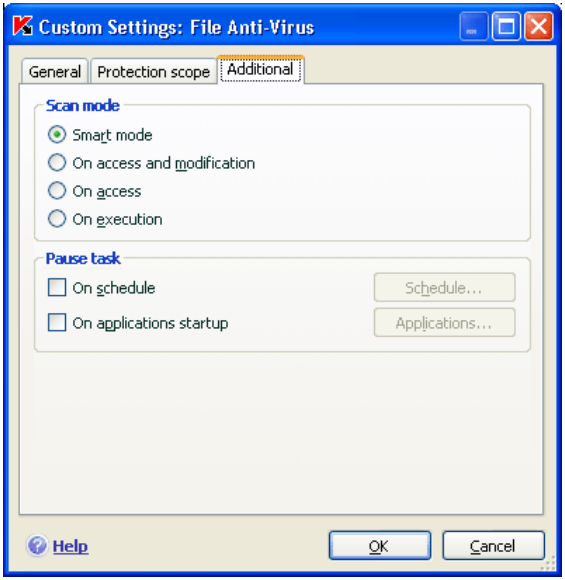


Figure 20. Configuring additional File Anti-Virus settings

The file scanning mode determines the File Anti-Virus processing conditions. You have following options:

- **Smart mode**. This mode is aimed at speeding up file processing and return them to the user. When it is selected, a decision to scan is made based on analyzing the operations performed with t he file.

  For example, when using a Microsoft Office file, Kaspersky Anti-Virus scans the file when it is first opened and last closed. All operations in between that overwrite the file are not scanned.

  Smart mode is the default.

- **On access and modification** – File Anti-Virus scans files as they are opened or edited.
- **On access** – only scans files when an attempt is made to open them.
- **On execution** – only scans files when an attempt is made to run them.

You might need to pause File Anti-Virus when performing tasks that require significant operating system resources. To lower the load and ensure that the user regains access to files quickly, we recommend configuring the component to disable at a certain time or while certain programs are used.

To pause the component for a certain length of time, check **On schedule** and in the window that opens (see Figure 21) click **Schedule** to assign a time frame for disabling and resuming the component. To do so, enter a value in the format HH:MM in the corresponding fields.

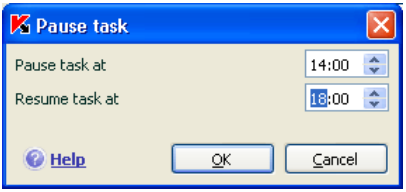


Figure 21. Pausing the component

To disable the component when working with programs that require significant resources, check **On applications startup** and edit the list of programs in the window that opens (see Figure 22) by clicking **Applications**.

To add an application to the list, use the **Add** button. A context menu will open, and by clicking **Browse** you can go to the standard file selection window and specify the executable file the application to add. Or, go to the list of applications currently running from the **Applications** item and select the one you want.

To delete an application, select it from a list and click **Delete**.

You can temporarily disable the pause on File Anti-Virus when using a specific application. To do so, uncheck the name of the application. You do not have to delete it from the list.

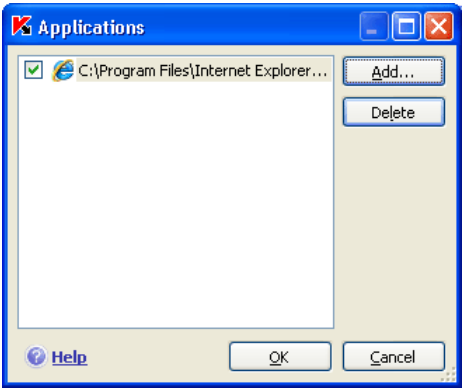


Figure 22. Creating an application list

7.2.4. Restoring default File Anti-Virus settings

When configuring File Anti-Virus, you can always return to the default performance settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

If you modified the list of objects included in the protected zone when configuring File Anti-Virus settings, the program will ask you if you want to save that list for future use when you restore the initial settings. To save the list of objects, check **Protected Zone** in the **Restore Settings** window that opens.

7.2.5. Selecting actions for objects

If File Anti-Virus discovers or suspects an infection in a file while scanning it for viruses, the program's next steps depend on the object's status and the action selected.

File Anti-Virus can label an object with one of the following statuses:

- Malicious program status (for example, *virus, Trojan*).

- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, all infected files are subject to disinfection, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings. All potential actions are displayed in the appropriate sections (see Figure 23).

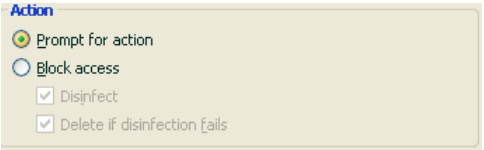


Figure 23. Possible File Anti-Virus actions with dangerous objects

If the action selected was	When it detects a dangerous object
Prompt for action	File Anti-Virus issues a warning message containing information about what malicious program has infected or potentially infected the file, and gives you a choice of actions. The choice can vary depending on the status of the object.
Block access	File Anti-Virus blocks access to the object. Information about this is recorded in the report (see 17.3 on pg. 224). Later you can attempt to disinfect this object.

If the action selected was	When it detects a dangerous object
Block access **Disinfect**	File Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If disinfection fails, the file will be assigned the status of *potentially infected*, and it will be moved to Quarantine (see 17.1 on pg. 218). Information about this is recorded in the report. Later you can attempt to disinfect this object.
Block access **Disinfect** **Delete if disinfection fails**	File Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup (see 17.2 on pg. 222).
Block access **Disinfect** **Delete**	File Anti-Virus will block access to the object and will delete it.

Before disinfecting or deleting the object, Kaspersky Anti-Virus for Windows Workstations creates a backup copy before it attempts to treat the object or delete it, in case the object needs to be restored or an opportunity arises to treat it.

7.3. Postponed disinfection

If you select **Block access** as the action for malicious programs, the objects will not be treated and access to them will be blocked.

If the actions selected were

Block access
Disinfect

all untreated objects will also be blocked.

In order to regain access to blocked objects, they must be disinfected. To do so:

1. Select **File Anti-Virus** in the main window of the program and left-click anywhere in the **Statistics** box.
2. Select the objects that interest you on the **Detected** tab and click the **Action** → **Treat all** button.

Successfully disinfected files will be returned to the user. Any that cannot be treated, you can *delete* or *skip* it. In the latter case, access to the file will be restored. However, this significantly increases the risk of infection on your computer. It is strongly recommended not to skip malicious objects.

CHAPTER 8. MAIL ANTI-VIRUS

Mail Anti-Virus is Kaspersky Anti-Virus for Windows Workstations' component for preventing incoming and outgoing email from transferring dangerous objects. It starts running when the operating system boots up, stays active in your system memory, and scans all email on protocols POP3, SMTP, IMAP, MAPI[1] and NNTP, as well as encrypted connections (SSL) for POP3 and IMAP (SSL).

The component's activity is indicated by the Kaspersky Anti-Virus for Windows Workstations system tray icon, which looks like this whenever an email is being scanned.

The default setup for Mail Anti-Virus is as follows:

1. Mail Anti-Virus intercepts each email received or sent by the user.
2. The email is broken down into its parts: email headers, its body, and attachments.
3. The body and attachments of the email (including OLE attachments) are scanned for dangerous objects. Malicious objects are detected using the *threat signatures* included in the program, and with the heuristic algorithm. The signatures contain descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the threat signatures.
4. After the virus scan, you have the following available courses of action:
    - if the body or attachments of the email contain malicious code, Mail Anti-Virus will block the email, place a copy of the infected object in *Backup*, and try to disinfect the object. If the email is successfully disinfected, it becomes available to the user again. If not, the infected object in the email is deleted. After the virus scan, special text is inserted in the subject line of the email stating that the email has been processed by Kaspersky Anti-Virus for Windows Workstations.
    - If code is detected in the body or an attachment that appears to be, but is not definitely. malicious, the suspicious part of the email is sent to *Quarantine*.

[1] Emails sent with MAPI are scanned using a special plug-in for Microsoft Office Outlook and The Bat!

- If no malicious code is discovered in the email, it is immediately made available again to the user.

A special plug-in (see 8.2.2 on pg. 104) is provided for Microsoft Outlook that can configure email scans more exactly.

If you use The Bat!, Kaspersky Anti-Virus for Windows Workstations can be used in conjunction with other anti-virus applications. The rules for processing email traffic (see 8.2.3 on pg. 105) are configured directly in The Bat! and supersede the Kaspersky Anti-Virus for Windows Workstations email protection settings.

Warning!

This version of Kaspersky Anti-Virus does not provide Mail Anti-Virus plug-ins for 64-bit mail clients.

When working with other email programs, including Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail, Mail Anti-Virus scans email on SMTP, POP3, IMAP, MAPI, and NNTP protocols.

Note that emails transmitted on IMAP are not scanned in Thunderbird if you use filters that move them out of your **Inbox**.

8.1. Selecting an email protection level

Kaspersky Anti-Virus for Windows Workstations protects your email at one of these levels (see Figure 24):

High – the level with the most comprehensive monitoring of incoming and outgoing emails. The program scans email attachments, including archives, in detail, regardless of how long the scan takes.

Recommended – Kaspersky Lab experts recommend this level. It scans the same objects as **High**, with the exception of attachments or emails that will take more than three minutes to scan.

Low – the security level with settings that let you comfortably use resource-intensive applications, since the scope of email scanning is limited. Thus, only your incoming email is scanned on this level, and in doing so archives and objects (emails) attached are not scanned if they take more than three minutes to scan. This level is recommended if you have additional email protection software installed on your computer.

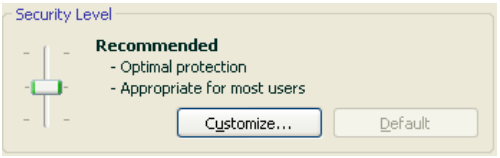


Figure 24. Selecting an email security level

By default, the email security level is set to **Recommended**.

You can raise or lower the email security level by selecting the level you want, or editing the settings for the current level.

To change the security level:

Adjust the sliders. By altering the security level, you define the ratio of scan speed to the total number of objects scanned: the fewer email objects are scanned for dangerous objects, the higher the scan speed.

If none of the preinstalled levels meets your needs, you can edit its settings. If you do, the level will be set to **Custom**. Let's look at an example of when user defined email security levels could be useful.

Example:

Your computer is outside the local area network and uses a dial-up Internet connection. You use Outlook Express as an email client for receiving and sending email, and you use a free email service. For a number of reasons, your email contains archived attachments. How do you maximally protect your computer from infection through email?

Tip for selecting a level:

By analyzing your situation, one can conclude that you are at a high risk of infection through email in the scenario outlined, because there is no centralized email protection and through using a dial-up connection.

You are advised to use **High** as your starting point, with the following changes: reduce the scan time for attachments to, for example, 1-2 minutes. The majority of archived attachments will be scanned for viruses and the processing speed will not be seriously slowed.

To modify the current security level settings:

Click the **Customize** button in the Mail Anti-Virus settings window. Edit the email protection settings in the window that opens, and click **OK**.

8.2. Configuring Mail Anti-Virus

A series of settings govern how your email is scanned. The settings can be broken down into the following groups:

- Settings that define the protected group (see 8.2.1 on pg. 102) of emails
- Email scan settings for Microsoft Outlook (see 8.2.2 on pg. 104) and The Bat! (see 8.2.3 on pg. 105)
- settings that define actions for dangerous email objects (see 8.2.4 on pg. 107)

The following sections examine these settings in detail.

8.2.1. Selecting a protected email group

Mail Anti-Virus allows you to select exactly what group of emails to scan for dangerous objects.

By default, the component protects email at the **Recommended** security level parameters, which means scanning both incoming and outgoing email. When you first begin working with the program, you are advised to scan outgoing email, since it is possible that there are worms on your computer that use email as a channel for distributing themselves. This will help avoid the possibility of unmonitored mass mailings of infected emails from your computer.

If you are certain that the emails that you are sending do not contain dangerous objects, you can disable the outgoing email scan. To do so:

1. Select **Mail Anti-Virus** in the main window and go to the component settings window by clicking Settings. Click on the **Customize** button in the Mail Anti-Virus configuration window.
2. In the **Custom Settings: Mail Anti-Virus** window (see Figure 25), select **Only incoming email** in the **Scope** section.

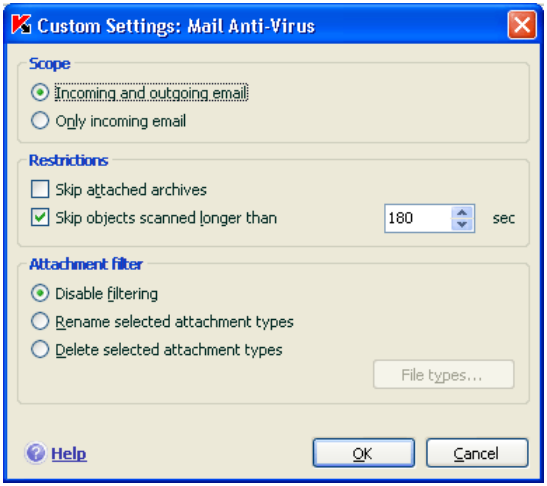


Figure 25. Mail Anti-Virus settings

In addition to selecting an email group, you can specify whether archived attachments should be scanned, and also set the maximum amount of time for scanning a single email object. These settings are configured in the **Restrictions** section.

If your computer is not protected by any local network software, and accesses the Internet without using a proxy server or firewall, you are advised **not to disable** the archived attachment scan and not to set a time limit on scanning.

If you are working in a protected environment, you can change the time restrictions on scanning to increase the email scan speed.

You can configure the filtration conditions for objects connected to an email in the **Attachment filter** section:

- **Disable filtering** – do not use additional filtration for attachments.
- **Rename selected attachment types** – filter out a certain attachment format and replace the last character of the file name with an underscore. You can select the file type by clicking the File types button.
- **Delete selected attachment types** – filter out and delete a certain attachment format. You can select the file type by clicking the File types button.

You can find more information about filtered attachment types in section A.1 on pg. 302.

By using the filter, you increase your computer's security, since malicious programs spread through email most frequently as attachments. By renaming or deleting certain attachment types, you protect your computer against automatically opening attachments when a message is received.

8.2.2. Configuring email processing in Microsoft Office Outlook

If you use Outlook as your email client, you can set up custom configurations for virus scans.

A special plug-in is installed in Outlook when you install Kaspersky Anti-Virus for Windows Workstations. It can quickly access Mail Anti-Virus settings, and also set the maximum time that individual emails will be scanned for dangerous objects.

Warning!

This version of Kaspersky Anti-Virus does not provide Mail Anti-Virus plug-ins for 64-bit Microsoft Office Outlook.

The plug-in comes in the form of a special **Mail Anti-Virus** tab located under **Service → Options** (see Figure 26).

Select an email scan mode:

- **Scan upon receiving** – analyzes each email when it enters your Inbox.
- **Scan when read** – scans each email when you open it to read it.
- **Scan upon sending** – scans each email for viruses when you send it.

Warning!

If you use Outlook to connect to your email service on IMAP, you are advised not to use **Scan upon receiving** mode. Enabling this mode will lead to emails being copied to the local computer when delivered to the server, and consequently the main advantage of IMAP is lost – creating less traffic and dealing with unwanted email on the server without copying them to the user's computer.

The action that will be taken on dangerous email objects is set in the Mail Anti-Virus settings, which can be configured by following the click here link in the **Status** section.

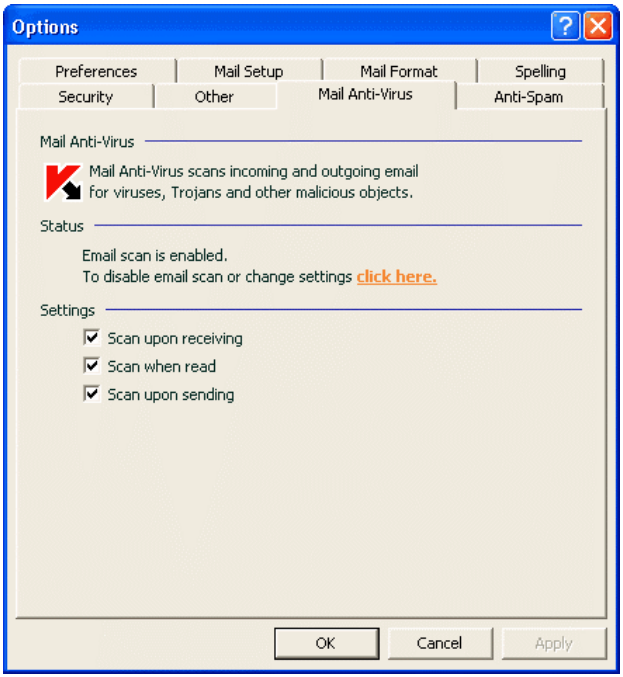


Figure 26. Configuring Mail Anti-Virus settings in Microsoft Outlook

8.2.3. Configuring email scans in The Bat!

Actions taken on infected email objects in The Bat! are defined with the program's own tools.

> Warning!
>
> The Mail Anti-Virus settings that determine whether incoming and outgoing email is scanned, as well as actions on dangerous email objects and exclusions, are ignored. The only settings that The Bat! takes into account relate to scanning archived attachments and time limits on scanning emails (see 8.2.1 on pg. 102).
>
> This version of Kaspersky Anti-Virus does not provide Mail Anti-Virus plug-ins for 64-bit The Bat!

To set up email protection rules in The Bat!:

1. Select **Settings** from the email client's **Properties** menu.
2. Select **Virus protection** from the settings tree.

The protection settings displayed (see Figure 27) extend to all anti-virus modules installed on the computer that support The Bat!

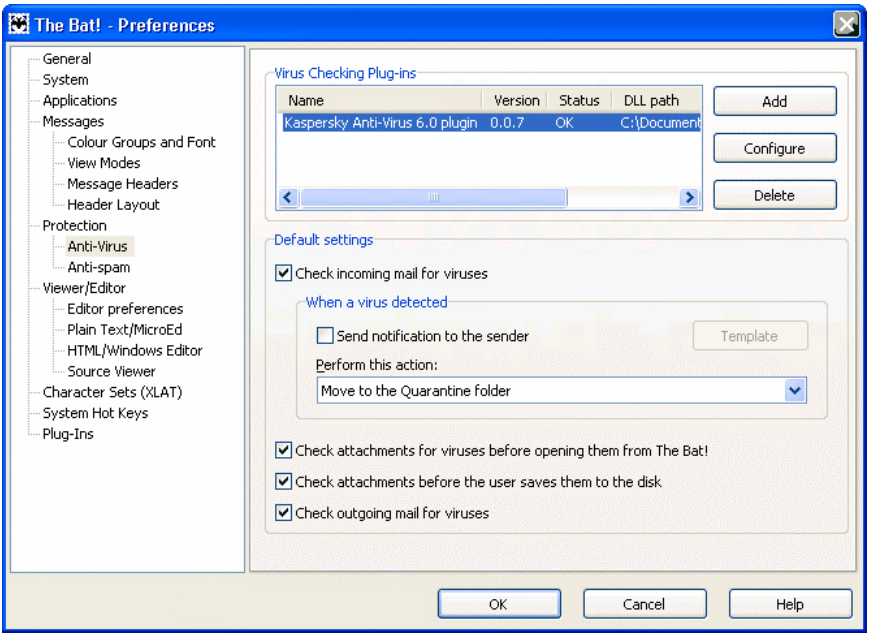


Figure 27. Configuring email scans in The Bat!

You must decide:

- What group of emails will be scanned for viruses (incoming, outgoing)
- At what point in time email objects will be scanned for viruses (when opening an email or before saving one to disk)
- The actions taken by the email client when dangerous objects are detected in emails. For example, you could select:

  Attempt to disinfect infected parts – tries to treat the infected email object, and if the object cannot be disinfected, it stays in the email. Kaspersky Anti-Virus for Windows Workstations will always inform you if an email is infected. But even if you select **Delete** in the Mail Anti-Virus notice window, the object will remain in the email, since the action selected in The Bat! takes precedent over the actions of Mail Anti-Virus.

  Delete infected parts – delete the dangerous object in the email, regardless of whether it is infected or suspected of being infected.

By default, The Bat! places all infected email objects in the Quarantine folder without treating them.

Warning!

The Bat! does not mark emails containing dangerous objects with special headers.

8.2.4. Restoring default Mail Anti-Virus settings

When configuring Mail Anti-Virus, you can always return to the default performance settings, which Kaspersky Lab considers to be optimal and has combined in the **Recommended** security level.

To restore the default Mail Anti-Virus settings:

1. Select **Mail Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

8.2.5. Selecting actions for dangerous email objects

If a scan shows that an email or any of its parts (body, attachment) is infected or suspicious, the steps taken by Mail Anti-Virus depend on the object status and the action selected.

One of the following statuses can be assigned to the email object after the scan:

- Malicious program status (for example, *virus, Trojan* – for more details, see 1.1 on pg. 11).
- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, when Mail Anti-Virus detects a dangerous or potentially infected object, it displays a warning on the screen and prompts the user to select an action for the object.

To edit an action for an object:

Open the Kaspersky Anti-Virus for Windows Workstations settings window and select **Mail Anti-Virus**. All possible actions for dangerous objects are listed in the **Action** box (see Figure 28).

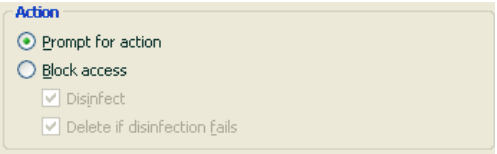


Figure 28. Selecting actions for dangerous email objects

Let's look at the possible options for processing dangerous email objects in more detail.

If the action selected was	When a dangerous object is detected
Prompt for action	Mail Anti-Virus will issue a warning message containing information about what malicious program has infected (potentially infected) the file and gives you the choice of one of the following actions.
Block access	Mail Anti-Virus will block access to the object. Information about this is recorded in the in the report (see 17.3 on pg. 224). Later you can attempt to disinfect this object.

If the action selected was	When a dangerous object is detected
Block access ☑ **Disinfect**	Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be treated, it is moved to Quarantine (see 17.1 on pg. 218). Information about this is recorded in the report. Later you can attempt to disinfect this object.
Block access ☑ **Disinfect** ☑ **Delete if disinfection fails**[2]	Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup. Objects with the status of potentially infected will be moved to Quarantine.
Block access ☐ **Disinfect** ☑ **Delete**	When Mail Anti-Virus detects an infected or potentially infected object, it deletes it without informing the user.

Before disinfecting or deleting an object, Kaspersky Anti-Virus for Windows Workstations creates a backup copy (see 17.2 on pg. 222) before it attempts to treat the object or delete it, in case the object needs to be restored or an opportunity arises to treat it.

[2] If you are using The Bat! as your mail client, dangerous email objects will either be disinfected or deleted when Mail Anti-Virus takes this action (depending on the action selected in The Bat!).

CHAPTER 9. WEB ANTI-VIRUS

Whenever you use the Internet, information stored on your computer is open to the risk of infection by dangerous programs, which can penetrate your computer when you read an article on the Internet.

Web Anti-Virus is Kaspersky Anti-Virus for Windows Workstations' component for guarding your computer during Internet use. It protects information that enters your computer via the HTTP protocol, and also prevents dangerous scripts from being loaded on your computer.

Warning!

Web Anti-Virus only monitors HTTP traffic that passes through the ports listed on the monitored port list (see 17.7 on pg. 245). The ports most commonly used for transmitting email and HTTP traffic are listed in the program package. If you use ports that are not on this list, add them to it to protect traffic passing through them.

If you are working on an unprotected network, or using a modem for Internet access, you are advised to use Web Anti-Virus to protect yourself while using the Internet. Even if your computer is running on a network protected by a firewall or HTTP traffic filters, Web Anti-Virus provides additional protection while you browse the Web.

The component's activity is indicated by the Kaspersky Anti-Virus for Windows Workstations system tray icon, which looks like this whenever scripts are being scanned.

Let's look at the component's operation in more detail.

Web Anti-Virus consists of two modules, that handle:

- *Traffic scan* – scans objects that enter the user's computer via HTTP.
- *Script scan* – scans all scripts processed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script, etc.) that are loaded while the user is on the computer.

  A special plug-in for Microsoft Internet Explorer is installed as part of Kaspersky Anti-Virus for Windows Workstations installation. The icon in the browser's Standard Buttons toolbar indicates that it is installed. Clicking on the icon opens an information panel with Web Anti-Virus statistics on the number of scripts scanned and blocked.

Web Anti-Virus guards HTTP traffic as follows:

1. Each web page or file that can be accessed by the user or by a certain program via HTTP is intercepted and analyzed by Web Anti-Virus for malicious code. Malicious objects are detected using both the threat signatures included in Kaspersky Anti-Virus for Windows Workstations, and the heuristic algorithm. The signatures contain descriptions of all malicious programs known to date, and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the threat signatures.
2. After the analysis, you have the following available courses of action:
    a. If the web page or object contains malicious code, the program blocks access to it, and a message appears on the screen, stating that the object or page is infected.
    b. If the file or web page does not contain malicious code, the program immediately grants the web browser access to it.

Scripts are scanned according to the following algorithm:

1. Web Anti-Virus intercepts each script run on a web page and scans them for malicious code.
2. If a script contains malicious code, Web Anti-Virus blocks it and informs the user with a special popup notice.
3. If no malicious code is discovered in the script, it is run.

Warning

Web Anti-Virus should be enabled before establishing the connection web-source to be able to intercept and check http-traffic and scripts if they contain viruses or not.

9.1. Selecting the web security level

Kaspersky Anti-Virus for Windows Workstations protects you while you use the Internet at one of the following levels (see Figure 29):

High – the level with the most comprehensive monitoring of scripts and objects incoming via HTTP. The program performs a thorough scan of all objects using the full set of threat signatures. This security level is recommended for aggressive environments, when no other HTTP security tools are being used.

Recommended – settings of this level are recommended by Kaspersky Lab experts. This level scans the same objects as **High**, but limits the

caching time for file fragments, thus accelerating the scan and returning objects to the user sooner.

Low – the security level with settings that let you comfortably use resource-intensive applications, since the scope of objects scanned is reduced by using a limited set of threat signatures. It is recommended to select this protection level if you have additional web protection software installed on your computer.

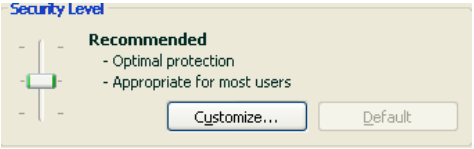


Figure 29. Selecting a web security level

By default, the protection level is set to **Recommended**.

You can raise or lower the security level by selecting the level you want or editing the settings for the current level.

To edit the security level:

Adjust the sliders. By altering the security level, you define the ratio of scan speed to the total number of objects scanned: the fewer objects are scanned for malicious code, the higher the scan speed.

If a preset level does not meet your needs, you can create a **Custom** security level. Let's look at an example of when such a level would be useful.

Example:

Your computer connects to the Internet via a modem. It is not on a corporate LAN, and you have no anti-virus protection for incoming HTTP traffic.

Due to the nature of your work, you regularly download large files from the Internet. Scanning files like these takes up, as a rule, a fair amount of time.

How do you optimally protect your computer from infection through HTTP traffic or a script?

Tip for selecting a level:

Judging from this basic information, we can conclude that your computer is running in a sensitive environment, and you are at high risk for infection through HTTP traffic, because there is no centralized web protection and due to the use of dial-up to connect to the Internet.

It is recommended that you use **High** as your starting point, with the following changes: you are advised to limit the caching time for file fragments during the scan.

To modify a preinstalled security level:

click the **Customize** button in the Web Anti-Virus settings window. Edit the web protection settings (see 9.2 on pg. 113) in the window that opens, and click **OK**.

9.2. Configuring Web Anti-Virus

Web Anti-Virus scans all objects that are loaded on your computer via the HTTP protocol, and monitors any WSH scripts (JavaScript, Visual Basic Script, etc.) run.

You can configure Web Anti-Virus settings to increase component operation speed, specifically:

- Set the scanning algorithm by selecting a complete or limited set of threat signatures
- Creating a list of trusted web addresses

It is also possible to select the actions that Web Anti-Virus will take in response to discovering dangerous HTTP objects.

The following sections examine these settings in detail.

9.2.1. Setting a scan method

You can scan data from the Internet using one of the following algorithms:

- *Streaming scan* – this method for detecting malicious code in network traffic scans data on the fly: as a file is downloading from the Internet, Web Anti-Virus scans the file's portions as they are downloaded, which delivers the scanned object to the user more quickly. At the same time, a limited set of threat signatures is used to perform streaming scans (only the most active threats), which significant lowers the security level for using the Internet.
- *Buffering scan* – this method scans objects only after they have been fully downloaded to the buffer. After the scan is complete, the program either passes the object to the user or blocks it.
  When using this scan type, the full threat signature set is used, which improves the level of malicious code detection. However, using this algorithm increases object processing time, and hence makes web

browsing slower: it can also cause problems when copying and processing large objects because the connection with the HTTP client can time out.

To select the scanning algorithm that Web Anti-Virus will use:

1. Click on the **Customize** button in the Web Anti-Virus configuration window.
2. In the window that opens (see Figure 30), select the option you want in the **Scan method** section.

By default, Web Anti-Virus performs a buffered scan on Internet data, and uses the complete threat signature set.

Warning!

If you encounter problems accessing resources like Internet radio, streaming video, or Internet conferencing, use streaming scan.

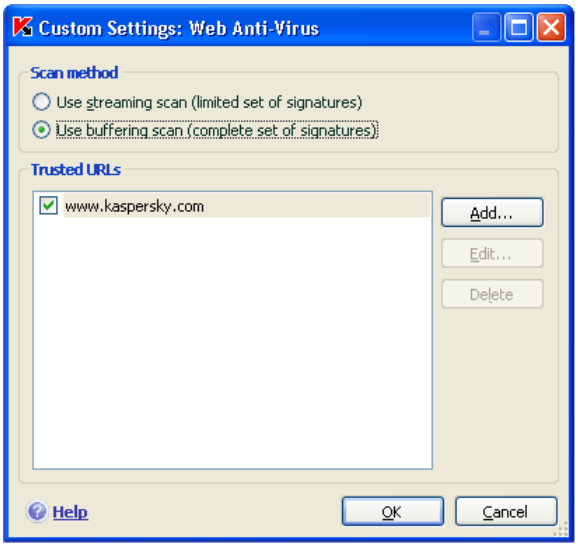


Figure 30. Configuring Web Anti-Virus

9.2.2. Creating a trusted address list

You have the option of creating a list of trusted addresses whose contents you fully trust. Web Anti-Virus will not analyze data from those addresses for

dangerous objects. This feature can be used if Web Anti-Virus hinders downloading a certain file by blocking an attempt to download it.

To create a list of trusted addresses:

1. Click on the **Customize** button in the Web Anti-Virus configuration window.
2. In the window that opens (see Figure 30), create a list of trusted servers in the **Trusted URLs** section. To do so, use the buttons to the right of the list.

When entering a trusted address, you can create masks with the following wildcards:

***** – any combination of characters.
Example: If you create the mask ***abc***, no URL contain **abc** will be scanned. For example: www.virus.com/download_virus/page_0-9abcdef.html

? – any single character.
Example: If you create mask **Patch_123?.com**, URLs containing that series of characters plus any single character following the 3 will not be scanned. For example: **Patch_1234.com** However, **patch_12345.com** will be scanned.

If an * or ? is part of an actual URL added to the list, when you enter them, you must use a backslash to override the * or ? following it.

Example: You want to add this following URL to the trusted address list: www.virus.com/download_virus/virus.dll?virus_name=

For Kaspersky Anti-Virus for Windows Workstations not to process **?** as a wildcard, put a backslash (\ )in front of it. Then the URL that you are adding to the exclusion list will be as follows:

www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Restoring default Web Anti-Virus settings

When configuring Web Anti-Virus, you can always return to the default performance settings, which Kaspersky Lab considers to be optimal and has combined as the **Recommended** security level.

To restore the default Web Anti-Virus settings:

1. Select **Web Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

9.2.4. Selecting responses to dangerous objects

If analyzing an HTTP object shows that it contains malicious code, the Web Anti-Virus response depends on the actions you select.

To configure Web Anti-Virus reactions to detecting a dangerous object:

Open the Kaspersky Anti-Virus for Windows Workstations settings window and select **Web Anti-Virus**. The possible responses for dangerous objects are listed in the **Action** section (see Figure 31).

By default, when a dangerous HTTP object is detected, Web Anti-Virus displays a warning on the screen and offers a choice of several actions for the object.

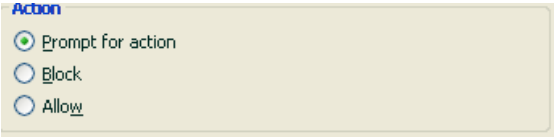


Figure 31. Selecting actions for dangerous scripts

The possible options for processing dangerous HTTP objects are as follows.

If the action selected was	If a dangerous object is detected in the HTTP traffic
Prompt for action	Web Anti-Virus will issue a warning message containing information about what malicious code has potentially infected the object, and will give you a choice of responses.
Block	Web Anti-Virus will block access to the object and will display a message on screen about blocking it. Similar information will be recorded in the report (see 17.3 on pg. 224).
Allow	Web Anti-Virus will grant access to the object. This information is logged in the report.

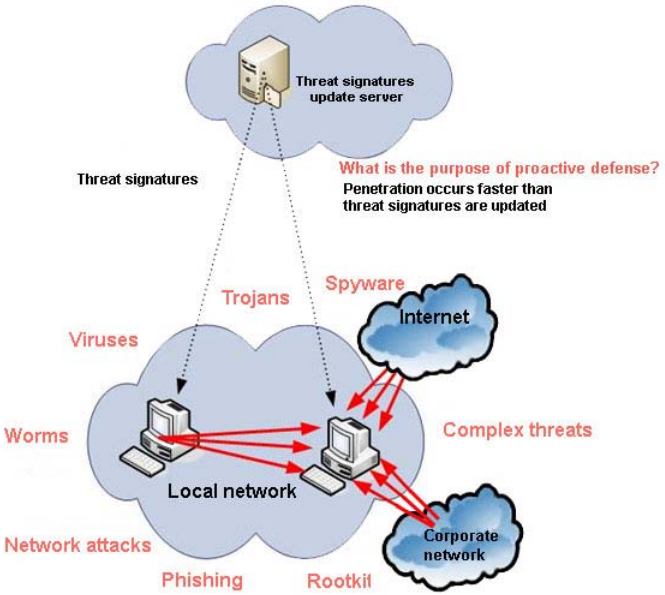
Web Anti-Virus always blocks dangerous scripts, and issues popup messages that inform the user of the action taken. You cannot change the response to a dangerous script, other than by disabling the script scanning module.

CHAPTER 10. PROACTIVE DEFENSE

Warning!

This version of the application does not have the proactive defense component **Office Guard** for computers running Microsoft Windows XP Professional x64 Edition or Vista or Microsoft Windows Vista x64.

Kaspersky Anti-Virus for Windows Workstations protects you both from known threats and from new ones about which there is no information in the threats signatures. This is ensured by a specially developed component – *Proactive Defense.*



The need for Proactive Defense has grown as malicious programs have begun to spread faster than anti-virus updates can be released to neutralize them.

The reactive technique, on which anti-virus protection is based, requires that a new threat infect at least one computer, and requires enough time to analyze the

malicious code, add it to the threat signatures and update the database on user computers. By that time, the new threat might have inflicted massive damages.

The preventative technologies provided by Kaspersky Anti-Virus for Windows Workstations Proactive Defense do not require as much time as the reactive technique, and neutralize new threats before they harm your computer. How is this done? In contrast with reactive technologies, which analyze code using threat signatures, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a given program. The application installation includes a set of criteria that can help determine how dangerous the activity of one program or another is. If the activity analysis shows that a certain program's actions are suspicious, Kaspersky Anti-Virus will take the action assigned by the rule for activity of the specific type.

Dangerous activity is defined by the overall actions of the program. For example, if actions such as a program copying itself to network resources, the startup folder, or the system registry, and then a number of copies of it are sent out, it is very likely that this program is a worm. Dangerous behavior also includes::

- Changes to the file system
- Modules being embedded in other processes
- Masking processes in the system
- Modification of certain Microsoft Window system registry keys

Proactive Defense tracks and blocks all dangerous operations by using the set of rules together with a list of excluded applications. Proactive Defense also tracks all macros executed in Microsoft Office applications.

Proactive Defense uses a set of rules included with the application, as well as user-defined rules created while using the application. A *Rule* is a set of criteria that defines suspicious behavior and how Kaspersky Anti-Virus reacts to it.

Individual rules are provided for application activity and monitoring changes to the system registry, macros, and programs run on the computer. You can alter the rules at your own discretion by adding, deleting, or editing them. Rules can block actions or grant permissions.

Let's examine the Proactive Defense algorithms:

1. Immediately after the computer is started, Proactive Defense analyzes the following factors, using the set of rules and exclusions:
    - *Actions of each application running on the computer*. Proactive Defense records a history of actions taken in order and compares them with sequences characteristic of dangerous activity (a database of dangerous activity types comes with the program and is updated with the threat signatures).

- *Actions of each VBA macro run* are analyzed for signs of malicious activity.
- *Each attempt to edit the system registry* by deleting or adding system registry keys, entering strange values for keys, etc.

2. Analysis is run based on Proactive Defense *allow* rules (according to the relevant criteria, the behavior is safe) and *block* rules (according to the relevant criteria, the behavior is malicious).
3. After the analysis, the following courses of action are available:
   - If the activity is not ruled as dangerous on the basis of the relevant criteria (*allow* and *block* rules), it is permitted.
   - If the activity is ruled as dangerous on the basis of the relevant criteria, the next steps taken by the component match the instructions specified in the rule: usually the activity is blocked. A message will be displayed on the screen specifying the dangerous program, its activity type, and a history of actions taken. You must accept the decision, block, or allow this activity on your own. You can create a rule for the activity and cancel the actions taken in the system.

10.1. Proactive Defense settings

The categories of settings (see Figure 32) for the Proactive Defense component are as follows:

- *Whether application activity is monitored on your computer*

  This Proactive Defense feature is enabled by checking the box ☑ **Enable Application Activity Analyzer**. By default this mode is enabled, which ensures that the actions of any programs opened on your computer will be closely tracked. A set of dangerous activities is highlighted for each of which you can configure the application processing procedure (see 10.1.1 on pg. 121) for that. You can also create Proactive Defense exclusions, which will stop the monitoring of selected applications.

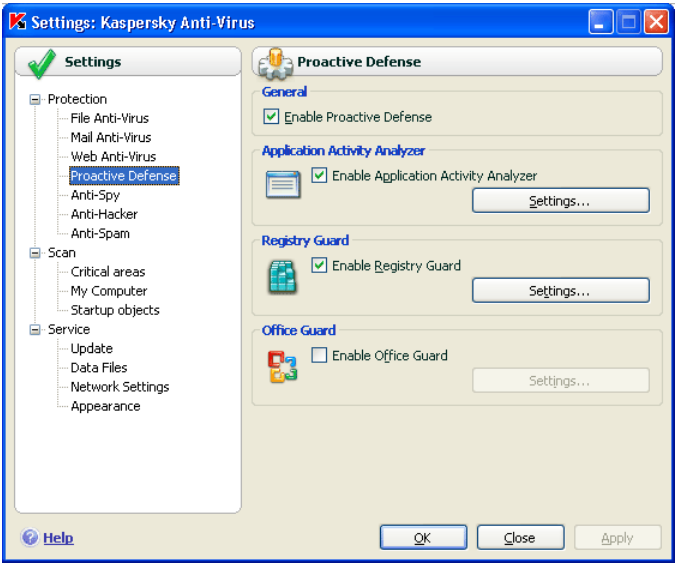


Figure 32. Proactive Defense settings

- Whether system registry changes are monitored

  By default, ☑ **Enable Registry Guard** is checked, which means Kaspersky Anti-Virus for Windows Workstations analyzes all attempts to make changes to the Windows system registry keys.

  You can create your own rules (see 10.1.3.2 on pg. 129) for monitoring the registry, depending on the Microsoft Windows registry key.

- Whether macros are scanned

  The monitoring of Visual Basic for Applications macros on your computer is controlled by checking the box ☑ **Enable Office Guard**, which is checked by default.

  You can select which macros are considered dangerous and what to do to them (see 10.1.2 on pg. 124).

> This Proactive Defense component is not available under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64.

You can configure exclusions (see 6.3.1 on pg. 72) for Proactive Defense modules and create a trusted application list (see 6.3.2 on pg. 77).

The following sections examine these aspects in more detail.

10.1.1. Activity control rules

Note that configuring application control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64 differs from the configuration process on other operating systems.

Information about configuring activity control for these operating systems is provided at the end of this section.

Kaspersky Anti-Virus monitors application activity on your computer. The application includes a set of event descriptions that can be tracked as dangerous. A monitoring rule is created for each such event. If the activity of any application is classified as a dangerous event, Proactive Defense will strictly adhere to the instructions stated in the rule for that event.

Select the **Enable Application Activity Analyzer** checkbox if you want to monitor the activity of applications.

Let's take a look a several types of events that occur in the system that the application will track as suspicious:

- *Dangerous behavior.* Kaspersky Anti-Virus analyzes the activity of applications installed on your computer, and based on the list of rules created by Kaspersky Lab, detects dangerous or suspicious actions by the programs. Such actions include, for example, masked program installation, or programs copying themselves.
- *Launching Internet browser with parameters*. By analyzing this type of activity, you can detect attempts to open a browser with settings. This activity is characteristic of opening a web browser from an application with certain command prompt settings: for example, when you click a link to a certain URL in an advertisement e-mail.
- *Intrusion into process (invaders)* – adding executable code or creating an additional stream to the process of a certain program. This activity is widely used by Trojans.
- *Hidden processes (rootkit)*. Rootkits are a set of programs used to mask malicious programs and their processes in the system. Kaspersky Anti-Virus analyzes the operating system for masked processes.
- *Window hooks*. This activity is used in attempts to read passwords and other confidential information displayed in operating system dialog boxes. Kaspersky Anti-Virus traces this activity if attempts are made to intercept data transferred between the operating system and the dialog box.
- *Suspicious values in registry*. The system registry is a database for storing system and user settings that control the operation of Windows, as

well as any utilities established on the computer. Malicious programs, attempting to mask their presence in the system, copy incorrect values in registry keys. Kaspersky Anti-Virus analyzes system registry entries for suspicious values.

- *Suspicious system activity*. The program analyzes actions executed by Microsoft Windows and detects suspicious activity. An example of suspicious activity would be an integrity breach, which involves modifying one or several modules in a monitored application since the time it was last run.
- *Keylogger detection*. This activity is used in attempts by malicious programs to read passwords and other confidential information which you have entered using your keyboard.
- *Microsoft Windows Task Manager protection*. Kaspersky Anti-Virus protects Task Manager from malicious modules injecting themselves into it when aimed at blocking Task Manager operation.

The list of dangerous activities can be extended automatically by the Kaspersky Anti-Virus for Windows Workstations update process, but it cannot be edited by the user. You can:

- Turn off monitoring for an activity by deselecting the ☑ next to its name
- Edit the rule that Proactive Defense uses when it detects a dangerous activity
- Create an exclusion list (see 6.3 on pg. 71) by listing applications that you do not consider dangerous.

To configure activity monitoring,

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Enable Application Activity Analyzer** section.

The types of activity that Proactive Defense monitors are listed in the **Settings: Application Activity Analyzer** window (see Figure 33).

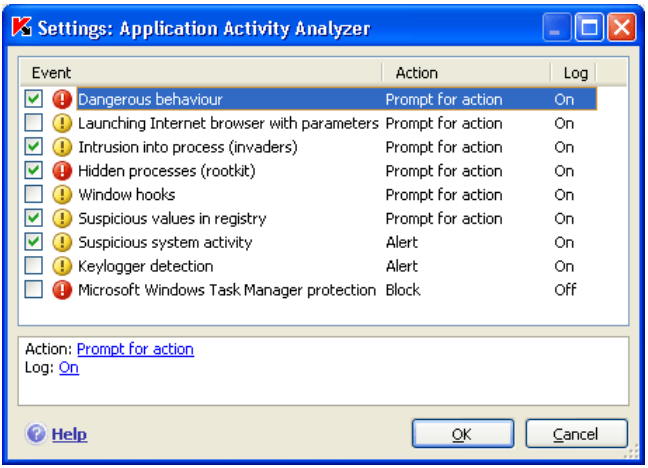


Figure 33. Configuring application activity control

To edit a dangerous activity monitoring rule, select it from the list and assign the rule settings in the lower part of the tab:

- Assign the Proactive Defense response to the dangerous activity.

  You can assign any of the following actions as a response: allow, prompt for action, and block. Left-click on the link with the action until it reaches the value that you need. In addition to stopping the process, you can place the application that initiated the dangerous activity in Quarantine. To do so, use the On / Off link across from the appropriate setting. You can assign a time value for how frequently the scan will run for detecting hidden processes in the system.

- Choose if you want to generate a report on the operation carried out. To do so, click on the **Log** link until it shows On or Off as required.

To turn off monitoring for a dangerous activity, uncheck the ☑ next to the name in the list.

Specifics of configuring application activity control in Kaspersky Anti-Virus under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64:

If you are running one of the operating systems listed above, only one type of system event is controlled, *dangerous behavior*. Kaspersky Anti-Virus for Windows Workstations analyses the activity of applications installed on the computer and detects dangerous or suspicious activities basing on the list of rules, created by Kaspersky Lab specialists.

If you want Kaspersky Anti-Virus to monitor the activity of system processes in addition to user processes, select the **Monitor system user accounts** checkbox (see Figure 34). This option is disabled by default.

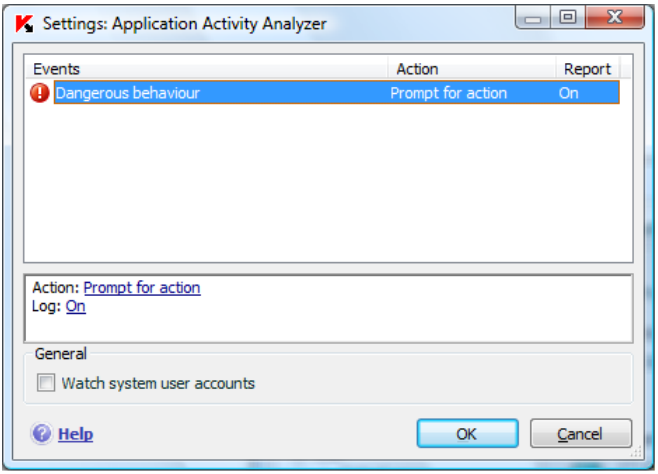


Figure 34. Configuring application activity control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

User accounts control access to the system and identify the user and his/her work environment, which prevents other users from corrupting the operating system or data. System processes are processes launched by system user accounts.

10.1.2. Office Guard

This Proactive Defense component does not work under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64.

You can enable scanning and processing of dangerous macros run on your computer by checking ☑ **Enable Office Guard**. Each macro run is scanned, and if it is on the list of dangerous macros, it is processed.

Example:

> The macro *PDFMaker* is a plug-in for the Adobe Acrobat toolbar in Microsoft Office Word that can create a .pdf file out of any document. Proactive Defense classifies embedding elements in software as a dangerous action. If Office Guard is enabled, when a macro is loaded Proactive Defense issues a warning on the screen, informing you that it has detected a dangerous macro command. You can choose to terminate that macro or allow it to continue.

You can configure what actions the program takes when macros engage in suspicious behavior. If you are sure that this macro is not dangerous when working with a specific file, for example, an MS Word document, we recommend creating an exclusion rule. If a situation arises that matches the terms of the exclusion rule, the suspicious action performed by the macro will not be processed by Proactive Defense.

To configure Office Guard:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Enable Office Guard** box.

Rules for processing dangerous macros are configured in the **Settings: Office Guard** window (see Figure 35) It contains default rules for behavior classified by Kaspersky Lab as dangerous, together with the response to be made by Proactive Defense. The actions of dangerous macros include, for example, embedding modules in programs and deleting files.

If you do not consider a behavior on the list to be dangerous, uncheck the box next to the name of the action. For example, you might frequently use macros to open files (not as read-only) and you are positive that this operation is not malicious.

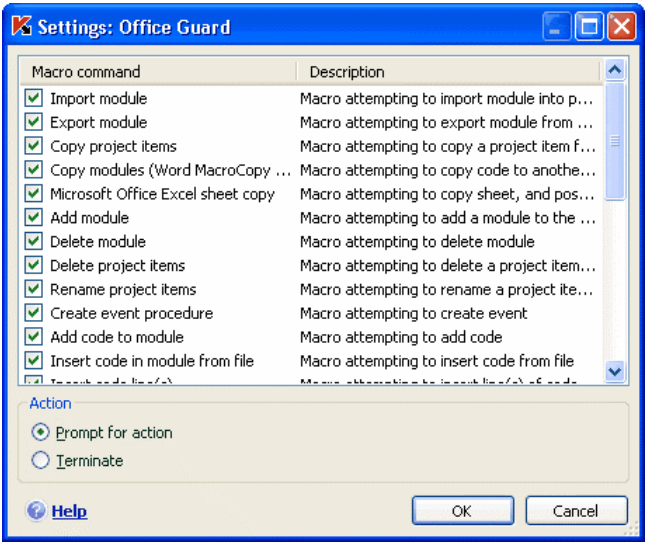

Settings: Office Guard
Macro command
Description
Import module
Macro attempting to import module into p...
Export module
Macro attempting to export module from ...
Copy project items
Macro attempting to copy a project item f...
Copy modules (Word MacroCopy ...
Macro attempting to copy code to anothe...
Microsoft Office Excel sheet copy
Macro attempting to copy sheet, and pos...
Add module
Macro attempting to add a module to the ...
Delete module
Macro attempting to delete module
Delete project items
Macro attempting to delete a project item...
Rename project items
Macro attempting to rename a project ite...
Create event procedure
Macro attempting to create event
Add code to module
Macro attempting to add code
Insert code in module from file
Macro attempting to insert code from file
Action
Prompt for action
Terminate
Help
OK
Cancel

Figure 35. Configuring Office Guard settings

For Kaspersky Anti-Virus for Windows Workstations not to block the macro:

uncheck the box next to that action. The program will no longer consider that behavior dangerous and Proactive Defense will not process it.

By default, whenever the program detects an action initiated by a macro on your computer, the application will ask you if you want to allow or block the macro.

In order for the program to automatically block all dangerous behavior without prompting the user:

In the window with the macro list, select **Terminate**.

10.1.3. Registry Guard

One of the goals of many malicious programs is to edit the Windows system registry on your computer. These can either be harmless jokes, or more malicious programs that present a serious threat to your computer.

For example, malicious programs can copy their information to the registry key that makes applications open automatically on startup. Malicious programs will then automatically be started when the operating system boots up.

To configure system registry monitoring:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Enable Registry Guard** section.

Kaspersky Lab has created a list of rules that control registry file operations, and have included it in the program. Operations with registry files are categorized into logical groups such as *System Security*, *Internet Security*, etc. Each such group lists system registry files and rules for working with them. This list is updated when the rest of the application is updated.

The **Settings: Registry Guard** window (see Figure 36) displays the complete list of rules.

Each group of rules has an execution priority that you can raise or lower, using the **Move Up** and **Move Down** buttons. The higher the group is on the list, the higher priority is assigned to it. If the same registry file falls under several groups, the first rule applied to that file will be the one from the group with the higher priority.

You can stop using any group of rules in the following ways:

- Uncheck the box ☑ next to the group's name. Then the group of rules will remain on the list but will not be used.
- Delete the group of rules from the list. We do not recommend deleting the groups created by Kaspersky Lab, since they contain a list of system registry files most often used by malicious programs.

You can create your own groups of monitored system registry files. To do so, click **Add** in the file group window.

Take these steps in the window that opens:

1. Enter the name of the new file group for monitoring system registry keys in the **Group name** field.
2. Select the **Keys** tab, and create a list of registry files that will be included in the monitored group (see 10.1.3.1 on pg. 128) for which you want to create rules. This could be one or several keys.
3. Select the **Rules** tab, and create a rule for files (see 10.1.3.2 on pg. 129) that will apply to the keys selected on the Keys tab. You can create several rules and set the order in which they are applied.

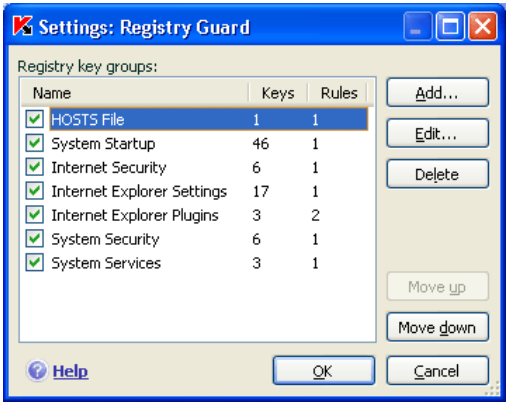


Figure 36. Controlled registry key groups

10.1.3.1. Selecting registry keys for creating a rule

The file group created should contain at least one system registry file. The **Keys** tab shows the list of files to which the rule(s) apply.

To add a system registry file:

1. Click on the **Add** button in the **Edit…** window (see Figure 37).
2. In the window that opens, select the registry file, or folder of files, for which you want to create the monitoring rule.
3. Specify an object value or mask for the group of objects, to which you want the rule to apply in the **Value** field.
4. Check **Including subkeys** for the rule to apply to all files attached to the listed registry file.

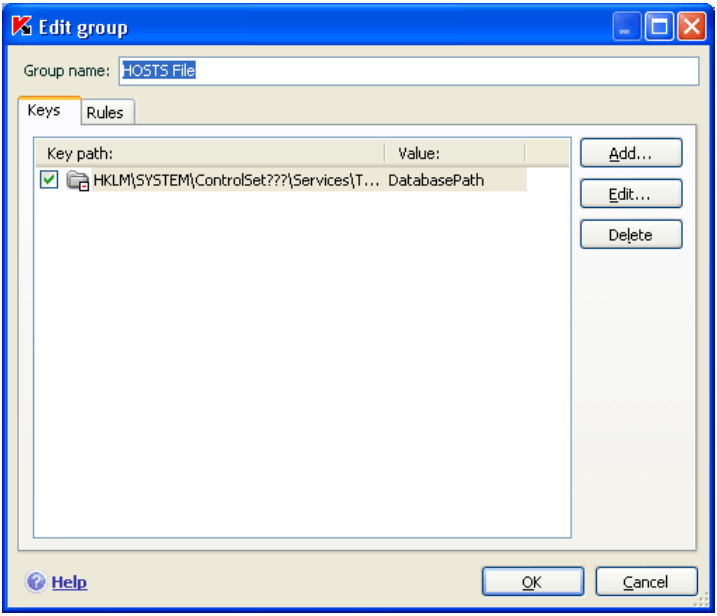


Figure 37. Adding controlled registry keys

You only need to use masks with an asterisk and a question mark at the same time as the **Include subkeys** feature if the wildcards are used in the name of the key.

If you select a folder of registry files using a mask and specify a specific value for it, the rule will be applied to that value for any key in the group selected.

10.1.3.2. Creating a Registry Guard rule

A Registry Guard rule specifies:

- The program whose access to the system registry is being monitored
- Proactive Defense's response when a program attempts to execute an operation with a system registry files

To create a rule for your selected system registry files:

1. Click **New** on the **Rules** tab. The new rule will be added at the top of the list (see Figure 38).

2. Select a rule on the list and assign the rule settings in the lower portion of the tab:

   - Specify the application.

     The rule is created for any application by default. If you want the rule to apply to a specific application, left-click on any and it will change to this. Then click on the specify application name link. A context menu will open: click **Browse** to see the standard file selection window, or click **Applications** to see a list of open applications, and select one of them as necessary.

   - Define the Proactive Defense response to the selected application attempting to read, edit, or delete system registry files.

     You can use any of these actions as a response: allow, prompt for action, and block. Left-click on the link with the action until it reaches the value that you need.

   - Choose if you want to generate a report on the operation carried out, by clicking on the log / do not log link.

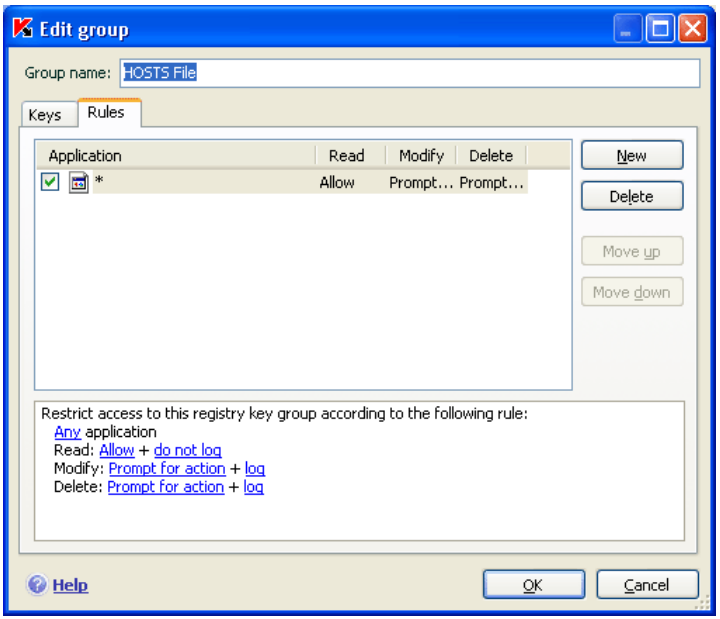


Figure 38. Creating an registry key monitoring rule

You can create several rules, and order their priority using the **Move Up** and **Move Down** buttons. The higher the rule is on the list, the higher the priority assigned to it will be.

You can also create an *allow* rule (i.e. all actions are allowed) for a system registry object from a notification window stating that a program is trying to execute an operation with an object. To do so, click Create allow rule in the notification and specify the system registry object that the rule will apply to in the window that opens.

CHAPTER 11. ANTI-SPY

The component of Kaspersky Anti-Virus for Windows Workstations which protects you against all types of malware is called *Anti-Spy*. Recently, malware has increasingly included programs that aim to:

- Steal your confidential information, including passwords, credit card numbers, important documents, etc.
- Track your actions on the computer and analyze the software installed on it.
- Deliver obtrusive advertising content in web browsers, popup windows, and banners in various programs.
- Gain unauthorized access to the Internet from your computer to various websites.

Phishing and keyloggers focus on stealing your information; autodialers, joke programs, and adware aim to waste your time and money. Protecting you from these programs is what Anti-Spy is designed to do.

Anti-Spy includes the following modules:

- The *Anti-Phishing* component protects you against phishing.

  Phishing generally consists of emails from supposed financial institutions, that contain links to their websites. The message text convinces the reader to click a link and enter confidential information into a web page, for example, a credit card number, or a login and password for an real Internet banking site.

  A common example of phishing is an email purporting to come from your bank, with a link to the official site. By clicking the link, you go to an exact copy of the bank's website and can even see the address in the browser's address bar, but are looking at page of a counterfeit site. From this point forward all actions which you take on the site are tracked and can be used to steal your money.

  You might receive a link to a phishing site via email, or through an instant messenger program. Anti-Phishing tracks attempts to open phishing sites and blocks them.

  The Kaspersky Anti-Virus for Windows Workstations threat signatures include the addresses of all phishing sites currently known. Kaspersky Lab specialists populate the list with addresses obtained from the Anti-Phishing Working Group, an international organization. Sites are added to the list by updating threat signatures.

- The *Popup Blocker* component blocks popup windows containing adverts with links to various websites.

  The information in these windows is generally not of benefit to you. These windows open automatically when you open a certain website, or go to a different window using a hyperlink. They contain advertisements and other information that you did not request. The Popup Blocker component blocks these windows, and a special message above the system tray icon informs you about it. You can determine directly in this message if you want to block the window or not.

  > Popup Blocker works correctly with the popup blocking module in Microsoft Internet Explorer included in Service Pack 2 for Microsoft Windows XP. When you install Kaspersky Anti-Virus for Windows Workstations, a plug-in is installed in the browser that lets you allow popup windows directly from the browser.

  Some sites use popup windows legitimately, to deliver information more quickly and conveniently. If you use such sites frequently and the popup windows are important to you, you can add them to the trusted sites list (see 11.1.1 on pg. 134) so that their popup windows will not be blocked.

  When using Microsoft Internet Explorer, the icon will appear in the browser status bar when a popup window is blocked. You can unblock it or add the address to the trusted address list by clicking on the icon.

- The *Anti-Banner* component blocks banner ads either on web pages, or built into the interfaces of programs installed on your computer.

  Banner ads are not just devoid of useful information, but also distract you from your work and increase the amount of traffic on your computer. Anti-Banner blocks the most common banner ads, based on masks created by Kaspersky Anti-Virus for Windows Workstations. You can disable banner blocking or create your own lists of allowed and blocked banners.

  > To integrate Anti-Banner into **Opera**, add the following line to *standard_menu.ini*, section **[Image Link Popup Menu]**:
  >
  > Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations\opera_banner_deny.vbs", "//nologo %C"

- The *Anti-Dialer* component protects you against unauthorized modem connections.

  > Anti-Dialer runs on Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista, and Microsoft Windows Vista x64.

Dialers generally establish connections with specific websites, such as sites with pornographic material. Then you are forced to pay for expensive traffic that you never wanted or used. If you want to exclude a number from the blocked list, you must place it on the trusted numbers list (see 11.1.3 on pg. 138).

11.1. Configuring Anti-Spy

Anti-Spy protects you from all programs known to Kaspersky Lab which could steal your confidential information or money. You can configure the component more specifically by:

- Creating a list of trusted websites (see 11.1.1 on pg. 134) whose popup windows you do not want to block
- Creating “black” and “white” lists of banners (see 11.1.2 on pg. 136)
- Creating trusted telephone number lists (see 11.1.3 on pg. 138) for dial-up connections that you allow

11.1.1. Creating Popup Blocker trusted address list

By default, Popup blocker blocks the majority of automatic popup windows. The exception is popup windows from websites on the trusted site list in Microsoft Internet Explorer, and Intranet sites that you currently a part of.

If you are running Windows XP with Service Pack 2, Internet Explorer already has its own popup blocker, which you can configure, selecting which particular windows you want to block and which you do not. Popup blocker is compatible with this blocker, using the following principle: a blocking rule takes precedence, that is, if either Internet Explorer or Popup blocker has a blocking rule for a popup window, the window is blocked. For this reason, we recommend configuring the browser and Popup Blocker together if you run Microsoft Windows XP Service Pack 2.

If you want to view a popup window for any reason, you must add it to the trusted address list. To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window and select Anti-Spy in the settings tree.
2. Click **Trusted sites** in the **Enable Popup Blocker** section.
3. Click **Add** in the window that opens (see Figure 39) and enter a mask for sites whose popup windows you do not want to block.

Tip:

When entering a trusted address mask, you can use the characters * or **?**.

For example, the mask http://www.test* excludes popups from any site that begins with that series of characters.

4. Specify if addresses in the Internet Explorer trusted zone or addresses on your local area network will be excluded from the scan. The program considers them trusted by default and does not block pop-up windows from these addresses.

The new exclusion will be added at the top of the trusted address list. To stop using the exclusion that you have added, just uncheck the box ☑ next to its name. If you want to remove an exclusion entirely, select it on the list and click **Delete**.

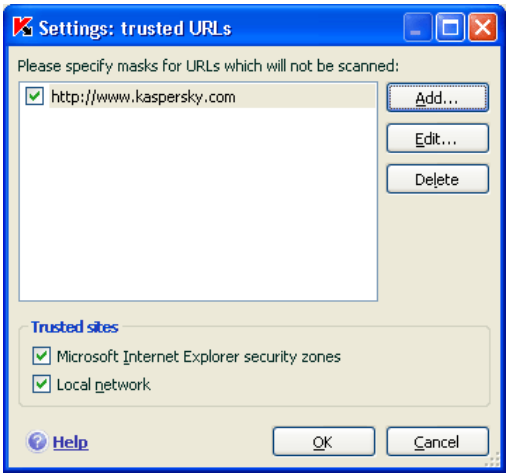


Figure 39. Creating an list of trusted addresses

If you want to block popups from your intranet or websites included in the Microsoft Internet Explorer list of trusted sites, uncheck the corresponding boxes in the **Trusted sites** section.

When popup windows that are not on the trusted address list try to open, a message appears over the program icon stating that it has blocked the window. There are links in the message that allow you to cancel the block and add the window's address to the trusted address list.

You can also unblock windows through Internet Explorer if you have Windows XP Service Pack 2. To do so, use the context menu that you can open over the

program icon that flashes in the bottom corner of the browser when popup windows are blocked.

11.1.2. Banner ad blocking list

Anti-Banner is the Kaspersky Anti-Virus for Windows Workstations component responsible for blocking banner adverts. Kaspersky Lab specialists have compiled a mask list of the most common banner ads, based on specially conducted research, and have included it with the program. If Anti-Banner is not disabled, it blocks banner ads that are selected by the masks on this list.

You can also create white and black lists for banner ads which will allow or block banner ads.

Note that if the blocked banners list or black list contains a mask for filtering domains, you will still be able to access the root site.

For example, if the blocked banner list includes a mask for **truehits.net**, you will be able to access **http://truehits.net**, but access to **http://truehits.net/a.jpg** will be blocked.

11.1.2.1. Configuring the standard banner ad blocking list

Kaspersky Anti-Virus for Windows Workstations includes a list of masks for the most common banner ads on websites and program interfaces. This list is compiled by Kaspersky Lab specialists and is updated along with the threat signatures.

You can select which standard banner ad masks you want to use when using Anti-Banner. To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window and select Anti-Spy in the settings tree.
2. Click the **Settings** button in the Anti-Banner section.
3. Open the **General** tab (see Figure 40). Anti-Banner will block the banner ad masks listed on the tab. You can use wildcards anywhere in a banner address.

The list of standard blocked masks cannot be edited. If you do not want to block a banner covered by a standard mask, uncheck the box ☑ next to the mask.

To analyze banner ads that do not match the masks from the standard list, check ☑ **Use heuristic analysis methods**. Then the application will analyze the

images loaded for signs typical of banner ads. Pursuant to this analysis, the image might be identified as a banner and blocked.

You can also create your own lists of allowed and blocked banners. You can do so on the **White list** and **Black list** tabs.

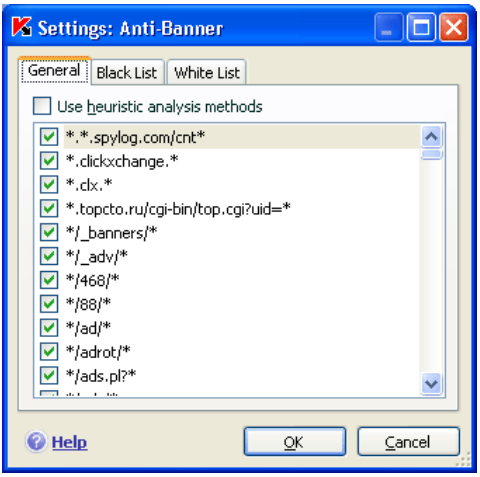


Figure 40. Blocked banner list

11.1.2.2. Banner ad white lists

You can create a banner ad white list to allow certain banners to be displayed. This list contains masks for allowed banner ads.

To add to a new mask to the white list:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window and select Anti-Spy in the settings tree.
2. Click the **Settings** button in the Anti-Banner section.
3. Open the **White list** tab.

Add the allowed banner mask with the **Add** button. You can specify the whole URL for the banner or a mask for it. In the latter case, when a banner attempts to load, the program will scan its address for the mask.

When creating a mask, you can use the wildcards ***** or **?** (where * represents a sequence of characters and ? – any one character).

To stop using a mask that you created, you can either delete it from the list, or uncheck the box ☑ next to it. Then banners that fall under this mask will revert to being blocked.

Using the **Import** and **Export** buttons, you can copy the list of allowed banners from one computer to another.

11.1.2.3. Banner ad black lists

In addition to the standard list of banners blocked (see 11.1.2.1 on pg. 136) by Anti-Banner, you can create your own list. To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window and select Anti-Spy in the settings tree.
2. Click the **Settings** button in the blocked banners section.
3. Open the **Black list** tab.

Using the **Add** button, enter a mask for the banner that you want Anti-Banner to block. You can specify the whole URL for the banner or a mask for it. In the latter case, when a banner attempts to load, the program will scan its address for the mask.

When creating a mask, you can use the wildcards ***** or **?** (where * represents a sequence of characters and ? – any one character).

To stop using a mask that you created, you can either delete it from the list, or uncheck the box ☑ next to it.

Using the **Import** and **Export** buttons, you can copy the list of blocked banners from one computer to another.

11.1.3. Creating an Anti-Dialer trusted number list

The *Anti-Dialer* component monitors telephone numbers used to secretly connect to the Internet. A connection is considered secret if it is configured not to inform the user of the connection, or if it is a connection that you do not initialize.

Whenever a secret connection is attempted, the program notifies you by issuing a special message on the screen, which prompts the user to either allow or block the phone call. If you did not initialize the connection, it is very probable that it was configured by a malicious program.

If you want to allow to make connections to certain numbers without being asked to confirm them every time, you must add them to the trusted number list. To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window and select Anti-Spy in the settings tree.
2. Click **Trusted numbers** in the Anti-Dialer section.
3. Click **Add** in the window that opens (see Figure 41) and enter a number or a mask for legitimate telephone numbers.

Tip:

When entering a trusted number mask, you can use the characters ***** or **?**.

For example, 0*???? 79787* will cover any numbers beginning with 79787 for which the area code is four digits.*

The new telephone number will be added at the top of the trusted number list. To stop using the number exclusion that you have added, just uncheck the box next to it on the list. If you want to remove an exclusion entirely, select it on the list and click **Delete**.

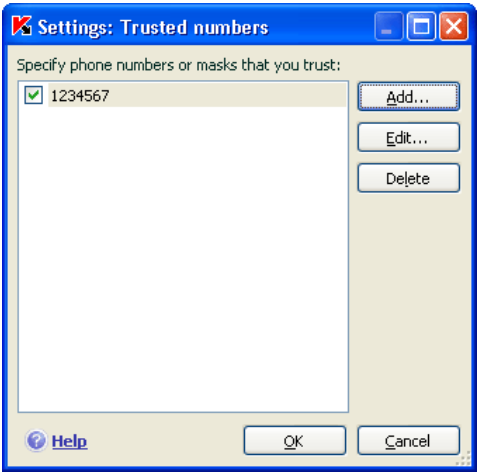
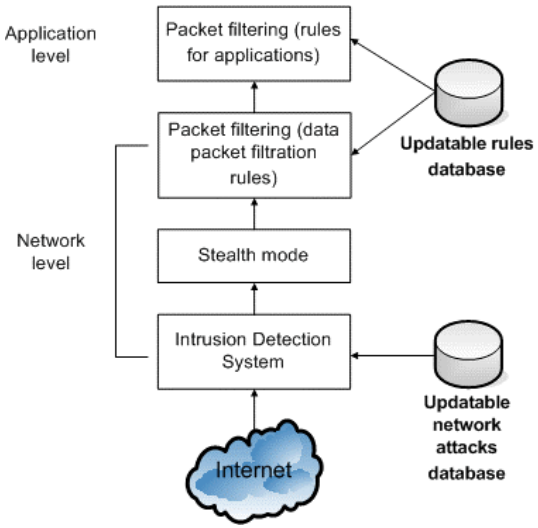


Figure 41. Creating a trusted address list

CHAPTER 12. PROTECTION AGAINST NETWORK ATTACKS

Today computers have become quite vulnerable when connected to the Internet. They are subjected both to virus infections and to other types of attacks that take advantage of vulnerabilities in operating systems and software.

The Kaspersky Anti-Virus for Windows Workstations *Anti-Hacker* component ensures your security on local networks and the Internet, by protecting your computer at the network and application levels, and masking your computer on the net to prevent attacks. Let's take a closer look at how Anti-Hacker works.



You are protected at the network level through global packet filtration rules, in which network activity is allowed or blocked, based on an analysis of settings such as: packet direction, the data transfer protocol, and the outbound packet port. Rules for data packets establish access to the network, regardless of the applications installed on your computer that use the network.

In addition to the packet filtration rules, the *Intrusion Detection System* (IDS) provides additional security at the network level. The goal of the IDS is to analyze inbound connections, detect port scans on your computer, and filter network packets aimed at exploiting software vulnerabilities. When running, the

IDS blocks all inbound connections from an attacking computer for a certain amount of time, and the user receives a message stating that his computer was subjected to an attempted network attack.

The Intrusion Detection System uses a special network attack database (see 12.9 on pg. 158) in analysis, which Kaspersky Lab expands regularly, and is updated together with the threat signatures.

Your computer is protected at the application level by making your computer's installed applications follow Anti-Hacker's application rules for the use of network resources. Similarly to the network security level, the application level security is built on analyzing data packets for direction, transfer protocol, and what ports they use. However, at the application level, both data packet traits and the specific application that sends and receives the packet are taken into account.

Using application rules helps you to configure specific protection allowing, for example, a certain connection type to be banned for some applications but not for others.

There are two Anti-Hacker rule types, based on the two Anti-Hacker security levels:

- *Packet filtering rules* (see 12.3 on pg. 147). Used to create general restrictions on network activity, regardless of the applications installed. Example: if you create a packet filtering rule that blocks inbound connections on port 21, no applications that use that port (an ftp server, for example) will be accessible from the outside.
- *Application rules* (see 12.2 on pg. 143). Used to create restrictions on network activity for specific applications. Example: If connections on port 80 are blocked for each application, you can create a rule that allows connections on that port for Firefox only.

There are two types of application and packet filtering rules: *allow* and *block*. The program installation includes rules which regulate network activity for the commonest applications and using the commonest protocols and ports. Kaspersky Anti-Virus for Windows Workstations also includes a set of allow rules for trusted applications whose network activity is not suspect.

Kaspersky Anti-Virus for Windows Workstations breaks down the entire network space into zones to make settings and rules more user-friendly: *Internet* and *security zones*, which largely correspond to the subnets that your computer belongs to. You can assign a status to each zone (*Internet, Local Area Network, Trusted*), which determine the policy for applying rules and monitoring network activity in that zone (see 12.5 on pg. 153).

A special feature of Anti-Hacker, *Stealth Mode*, prevents the computer from being detected from the outside, so that hackers cannot detect the computer to attack it. This mode does not affect your computer's performance on the Internet:

you are advised not to use Stealth Mode if your computer is functioning as a server.

12.1. Selecting an Anti-Hacker security level

When you use the network, Kaspersky Anti-Virus for Windows Workstations protects your computer at one of the following levels (see Figure 42):

Enable Firewall
Low Security
Allow the network activity of all applications except those explicitly prohibited by user-defined application rules.
Settings...

Figure 42. Selecting an Anti-Hacker security level

High Security – passes only allowed network activity, using allow rules that either came with the program or that you created. The set of rules included with Kaspersky Anti-Virus for Windows Workstations includes allow rules for applications whose network activity is not suspicious, and for data packets that are absolutely safe to send and receive. However, if there is a block rule with a higher priority than the allow rule, the program will block the network activity of that application.

> Warning!
>
> If you select this security level, any network activity not recorded in an Anti-Hacker allow rule will be blocked. Therefore we recommend only using this level if you are certain that all the programs you need are allowed by the rules to make network connections, and that you do not plan on installing new software.

Training mode – protection level where Anti-Hacker rules are created. At this level, whenever a program attempts to use a network resource, Anti-Hacker checks to see if there is a rule for that connection. If there is a rule, Anti-Hacker applies it. If there is no rule, a message will appear on the screen, containing a description of the network connection (what program initiated it, what port, the protocol, etc.). You must decide whether to allow this connection or not. Using a special button in the message window, you can create a rule for that connection, so that in the future Anti-Hacker will apply the new rule for that connection without warning you on screen.

Low Security – blocks only banned network activity, using block rules that either were installed by with the program or that you created. However, if there is a allow rule for an application with a higher priority than the block rule, the program will allow the network activity of that application.

Allow all – allows all network activity on your computer. You are advised to set protection to this level in extremely rare cases, when no active network attacks have been observed and you fully trust all network activity.

You can raise or lower the network security level by selected the existing level you want, or by changing the settings for the current level.

To modify the network security level:

1. Select **Anti-Hacker** in the Kaspersky Anti-Virus for Windows Workstations settings window.
2. Adjust the slider in the **Enable Firewall** section, to indicate the required security level.

To configure the network security level:

1. Select the security level that best matches your preferences, as above.
2. Click the **Settings** button and edit the network security settings in the window that opens.

12.2. Application rules

Kaspersky Anti-Virus for Windows Workstations includes a set of rules for the commonest Windows applications. These are programs whose network activity has been analyzed in detail by Kaspersky Lab, and is strictly defined as either dangerous or trusted.

Depending on the security level (see 12.1 on pg. 142) selected for the Firewall, and the type of network (see 12.5 on pg. 153) on which the computer is running, the list of rules for programs can be used in various ways. For example, with **Maximum protection** any application network activity that does not match the allow rules is blocked.

To work with the application rule list:

1. Click **Settings** in the Firewall section of the Anti-Hacker settings window.
2. In the window that opens, select the **Rules for applications** tab (see Figure 43).

The rules on this tab can be grouped in one of two ways:

- *Application rules* If **Group rules by application** is checked, then each application for which rules have been created will be shown on a single line in the list. The following information is given for every application: name and icon of the application, command prompt, root directory containing the application's executable file is, and the number of rules created for it.

  Using the **Edit** button, you can go to the list of rules for the application selected on the list and edit it: add a new rule, edit existing ones, and change their relative priority.

  Using the **Add** button, you can add a new application to the list and create a rule for it.

  The **Export** and **Import** buttons are designed to transfer the rules to other computers, which helps to configure Anti-Hacker quickly.

- *General list of rules* If **Group rules by application** is unchecked, then each line in the general list displays complete information for a rule: the application name and the command for starting it, whether to allow or block network activity, the data transfer protocol, the direction of data (inbound or outbound), and other information.

  Using the **Add** button, you can create a new rule, and you can alter an existing rule by selecting it on the list and clicking the **Edit** button. You can also edit the basic settings in the lower part of the tab.

  You can change their relative priority with the **Move up** and **Move down** buttons.

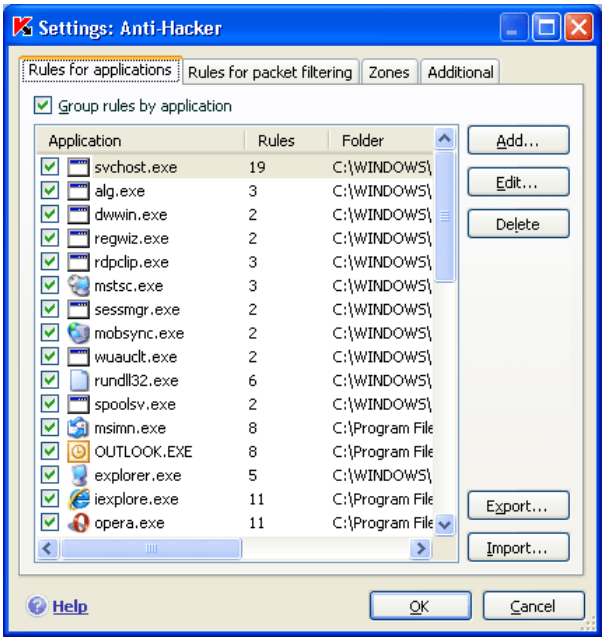


Figure 43. List of rules for the applications installed on a computer

12.2.1. Creating rules manually

To create an application rule manually:

1. Select the application. To do so, click the **Add** button on the **Rules for Applications** tab (see Figure 43). This will display a shortcut menu which will take you to a standard file selection dialog through its **Browse** option or to a list of running applications through its **Applications** option allowing you to make your selection. A list of rules for the application selected will open. If rules for it already exist, they will all be listed in the upper part of the window. If no rules exist, the rules window will be empty.
2. Click the **Add** button in the rules window for the selected application.

You can use the **New rule** window that opens to fine-tune a rule (see 12.6 on pg. 153).

12.2.2. Creating rules from template

Anti-Virus includes ready-made rule templates that you can use when creating your own rules.

The entire gamut of existent network application can be broken down into several types: mail clients, web browsers, etc. Each type is characterized by a set of specific activities, such as sending and receiving mail, or receiving and displaying html pages. Each type uses a certain set of network protocols and ports. This is why having rule templates helps to quickly and easily make initial configurations for rules based on the type of application.

To create an application rule from a template:

1. Check **Group the rules by application** on the **Application Rules** tab, if not checked already, and click the **Add** button.
2. This will display a shortcut menu which will take you to a standard file selection dialog through its **Browse** option or to a list of running applications through its **Applications** option allowing you to make your selection. This, in turn, will open a rules dialog for the selected application. Rules for the application will be displayed in the top part of the window. If no rules have been created, the window will be empty.
3. Click **Template** in the rules for applications window and select one of the rule templates from the context menu (see Figure 44).

   Allow all is a rule that allows all network activity for the application. **Block all** is a rule that blocks all network activity for the application. All attempts to initiate a network connection by the application in question will be blocked without notifying the user.

   Other templates listed on the context menu create rules typical for the corresponding types of program. For example, the **E-Mail Client** template creates a set of rules that allow standard network activity for email clients, such as sending email.

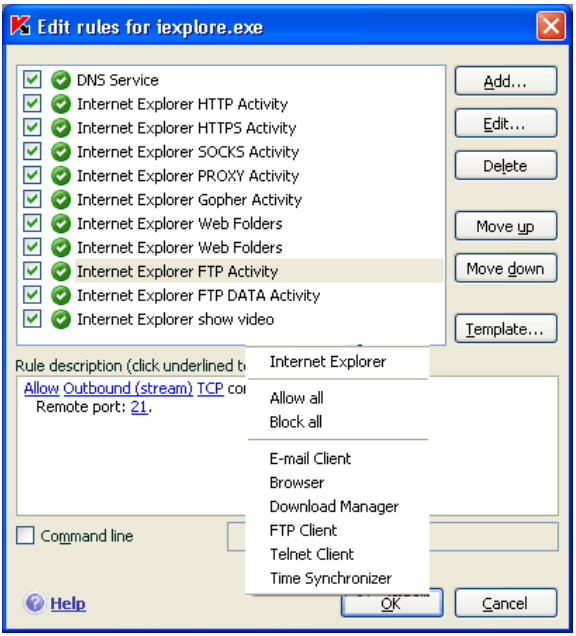


Figure 44. Selecting a template for creating a new rule

4. Edit the rules created for the application, if necessary. You can modify actions, network connection direction, remote address, ports (local and remote), and the time range for the rule.

5. If you want the rule to apply to a program opened with certain command line settings, check ☑ **Command line** and enter the string in the field to the right.

The rule or set of rules created will be added to the end of the list with the lowest ranking priority. You can raise the priority of the rule (see 12.5 on pg. 153).

You can create a rule from the network activity detection alert window (see 12.10 on pg. 161).

12.3. Packet filtering rules

Kaspersky Anti-Virus install package includes a set of rules that it uses to filter incoming and outgoing data packets for your computer. You can initiate data packet transfer or an installed program on your computer can. The program

includes filtering packet rules, devised by Kaspersky Lab, which determine whether data packets are dangerous or not.

Depending on the security level selected for the Firewall and the type of network the computer is running on, the list of rules can be used in various ways. Thus, for example, on the **High** level, all network activity not covered by allow rules is blocked.

Important!

Note that rules for security zones (see 12.6 on pg. 153) have higher priority than blocking packet rules. So, for example, if you select the status **Local Area Network**, packet exchanges will be allowed, and so will access to shared folders regardless of blocking packet rules.

To work with the list of packet filtering rules:

1. Click **Settings** in the Firewall section of the Anti-Hacker settings window.
2. In the window that opens, select the **Rules for packet filtering** tab (see Figure 45).

The following information is given for every packet filtering rule: name of the rule, the action (i.e. whether to allow or block the packet transfer), the data transfer protocol, the direction of the packet, and the network connection settings used to transfer the packet.

If the box beside the name of the rule is checked, the rule will be used.

You can work with the rule list using the buttons to the right of the list.

To create a new packet filtration rule:

Click the **Add** button on the **Rules for packet filtering** tab.

The **New rule** window that opens has a form that you can use to fine-tune a rule (see section 12.4 on pg. 149).

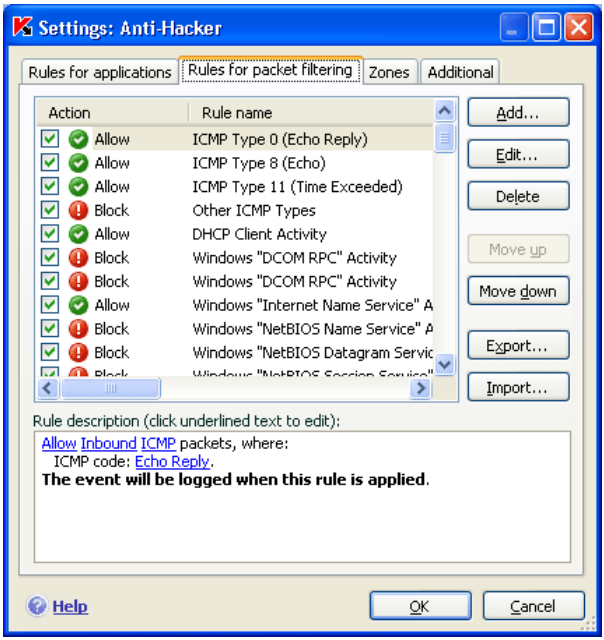


Figure 45. List of packet filtering rules

12.4. Fine-tuning rules for applications and packet filtering

The **New rule** window for advanced rule settings is practically identical for applications and data packets (see Figure 46).

Step One:

- Enter a name for the rule. The program uses a default name that you should replace.
- Select network connection settings for the rule: remote IP-address, remote port, local IP-address, and the time that the rule was applied. Check all the settings that you want to use in the rule.
- Configure settings for user notifications. If you want a popup message with a brief commentary to appear on the screen when a rule is used,

check **Display warning**. If you want the program to record invocations of the rule in the Anti-Hacker report, check **Log event**. The box is not checked by default when the rule is created. You are advised to use additional settings when creating block rules.

Note that when you a create a blocking rule in Anti-Hacker training mode, information about the rule being applied will automatically be entered in the report. If you do not need to record this information, deselected the **Log in report** checkbox in the settings for that rule.

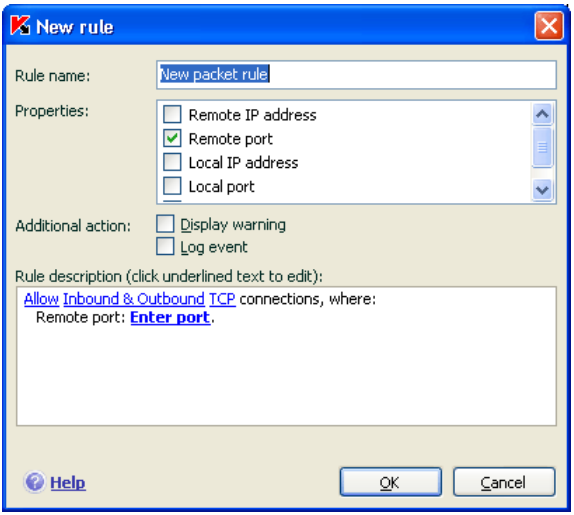


Figure 46. Creating a new application rule

Step Two in creating a rule is assigning values for rule parameters and selecting actions. These operations are carried out in the **Rule description** section.

1. The default action of every new rule is *allow*. To change it to a *block* rule, left-click on the Allow link in the rule description section. It will change to Block.

   Kaspersky Anti-Virus will still scan network traffic for programs and packets for which an allow rule as been created. This could result in data being transmitted more slowly.

2. If you did not select an application prior to creating the rule, you will need to do so by clicking select application. Left-click on the link and, in the standard file selection window that opens, select the executable file of the application for which you are creating the rule.

3. Determine the direction of the network connection for the rule. The default value is a rule for a bi-directional (both inbound and outbound) network connection. To change the direction, left-click on Inbound & outbound and select the direction of the network connection in the window that opens:

   - **Inbound stream**. The rule is applied to network connections opened by a remote computer.
   - **Inbound**. The rule applies to data packets received by your computer, except for TCP-packets.
   - **Inbound & outbound stream**. The rule is applied to inbound and outbound traffic regardless of which computer, the local one or the remote one, initiated the network connection.
   - **Outbound stream**. The rule is only applied to network connections opened by your computer.
   - **Outbound**. The rule is applied for inbound data packets that your computer sends, except for TCP-packets.

   If it is important for you to specifically set the direction of packets in the rule. Select whether they are inbound or outbound packets. If you want to create a rule for streaming data, select stream: inbound, outbound, or both.

   The difference between *stream direction* and *packet direction* is that when you create a rule for a stream, you define the direction of the connection. The direction of packets when transferring data on this connection is not taken into consideration.

   For example, if you configure a rule for data exchange with an FTP server that is running in passive FTP mode, you must allow an outbound stream. To exchange data with an FTP server in active FTP mode, you must allow both outbound and inbound streams.

4. If you selected a remote address as a network connection property, left-click specify the address and enter the IP address, a range of addresses or subnetwork address for the rule in the window that opens. You can use one type of IP address or several types for one rule. Several addresses of each type can be specified.

5. Set the protocol that the network connection uses. TCP is the default protocol for the connection. If you are creating a rule for applications, you can select one of two protocols, TCP or UDP. To do so, left-click on the link with the protocol name until it reaches the value that you need. If you are creating a rule for packet filtering and want to change the default protocol, click on its name and select the protocol you need in the window that opens. If you select ICMP, you may need to further indicate the type.

6. If you selected network connection settings (address, port, time range), you will have to assign them exact values as well.

After the rule is added to the list of rules for the application, you can further configure the rule (see Figure 47). If you want it to apply to an application opened with certain command line parameters, check **Command line** and enter the parameter string in the field to the right. This rule will not apply to applications started with a different command line.

You do not have the option of command line start settings in Microsoft Windows 98.

You can create a rule from the network activity detection alert window (see 12.10 on pg. 161).

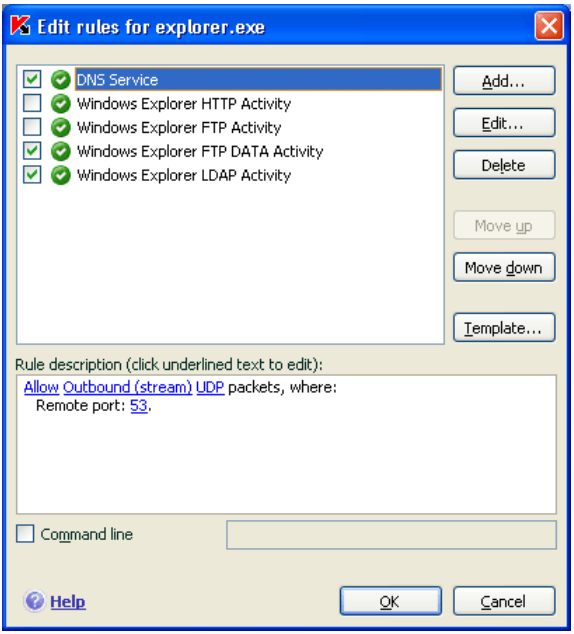


Figure 47. Advanced new rule settings

12.5. Ranking rule priority

Each application or package rule has an assigned execution priority. When other conditions are equal (for example, the network connection settings), the action applied to the program activity will be the rule with the higher priority.

The priority of a rule is determined by its position on the list of rules. The first rule on the list has the highest priority. Each rule created manually is added at the top of the list. Rules created from a template or from a notification are added at the bottom of the list.

To prioritize application rules, take the following steps:

1. Select the application name on the **Rules for applications** tab and click the **Edit** button.
2. Use the **Move up** and **Move down** buttons on the application rules tab to move rules on the list, changing their priority ranking.

To prioritize packet filtering rules, take the following steps:

1. Select the rule on the **Rules for Packet Filtering** tab.
2. Use the **Move up** and **Move down** buttons on the packet filtering tab to move rules on the list, thereby changing their priority ranking.

12.6. Rules for security zones

After you install Anti-Hacker on your computer, it analyzes your computer's network environment. Based on the analysis, it breaks down the entire network space into zones:

Internet – the World Wide Web. In this zone, Kaspersky Anti-Virus for Windows Workstations operates as a personal firewall, using default application and packet filtering rules to regulate all network activity and ensure maximum security. You cannot change protection settings when working in this zone, other than to enable Stealth Mode on your computer for added safety.

Security zones – certain conventional zones that mostly correspond with subnets that your computer is registered on (this could be local subnets at home or at work). These zones are usually average risk-level zones. You can change the status of these zones based on how much you trust a certain subnet, and you can configure appropriate rules for packet filtering and applications.

If Anti-Hacker Training Mode is enabled, a window will open every time your computer connects to a new zone, displaying a basic description about it. You

must assign a status to the zone, and network activity will be allowed based on that status. The possible values of the status are as follows:

- **Internet**. This is the default status assigned to the Internet, since when you are connected to it, your computer is subjected to all potential threat types. This status is also recommended for networks that are not protected by any anti-virus programs, firewalls, filters, etc. When you select this status, the program ensures maximum security while you are using this zone, specifically:
    - Blocking any network NetBios activity within the subnet
    - Blocking application and packet filtering rules that allow NetBios activity within this subnet

  Even if you have created a shared folder, the information in it will not be available to users from subnetworks with this status. Additionally, if this status is selected for a certain subnetwork, you will not be able to access files and printers of this subnetwork.
- **Local Area Network**. The program assigns this status to all zones detected when it analyzes the computer's network environment, except the Internet. This status is recommended for zones with an average risk factor (for example, corporate LANs). If you select this status, the program allows:
    - Any network NetBios activity within the subnet
    - Application and packet filtering rules that allow NetBios activity within this subnet

  Select this status if you want to grant access to certain folders or printers on your computer but block any other outside activity.
- **Trusted**. This status is only recommended for zones that you feel are absolutely safe, and where your computer will not be subject to attacks or invasions. If you select this status, all network activity is allowed. Even if Maximum Protection is selected and you have created block rules, they will not function for remote computers from a trusted zone.

  Note that any restrictions or access to files is only in effect without this subnet.

You can use Stealth Mode for added security when using a network designated as **Internet**. This feature only allows network activity initiated from your computer, so that your computer becomes invisible to its surroundings. This mode does not affect your computer's performance on the Internet.

We do not recommend using Stealth Mode if the computer is being used as a server (for example, an email or HTTP server), as the computers that connect to the server will not see it as connected.

The list of zones on which your computer is registered is displayed on the **Zones** tab (see Figure 48). Each of them is assigned a status, a brief description of the network, and whether Stealth Mode is used.

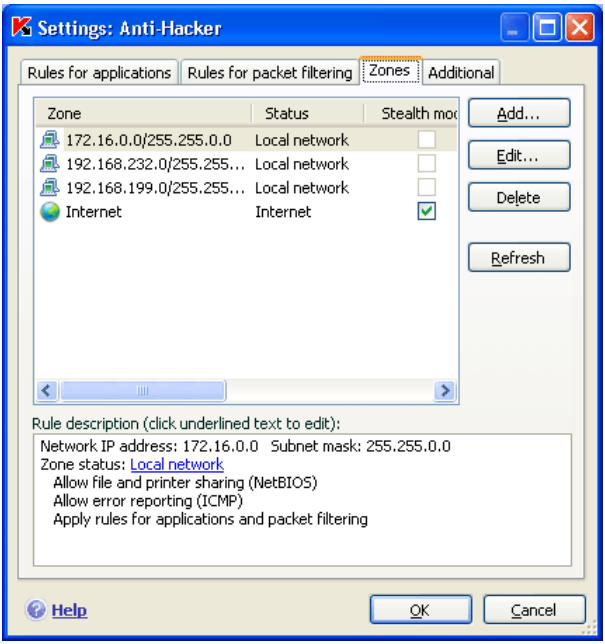


Figure 48. List of rules for zones

To change a zone's status, or to enable/disable Stealth Mode, select the zone from the list, and use the appropriate links in the **Rule Description** box below the list. You can perform similar tasks and edit addresses and subnet masks in the **Zone settings** window, which you can open by clicking **Edit**.

You can add a new zone to the list while viewing it. To do so, click **Refresh**. Anti-Hacker will search for potential zones to register, and if any are detected, the program will ask you to select a status for them. In addition, you can add new zones to the list manually (for example, if you connect your laptop to a new network). To do so, use the **Add** button and fill in the necessary information in the **Zone settings** window.

To delete a network from the list, select it in the list and click on the **Delete** button.

12.7. Firewall mode

The Firewall mode (see Figure 49) controls Anti-Hacker compatibility with programs that establish multiple network connections, and to network games.

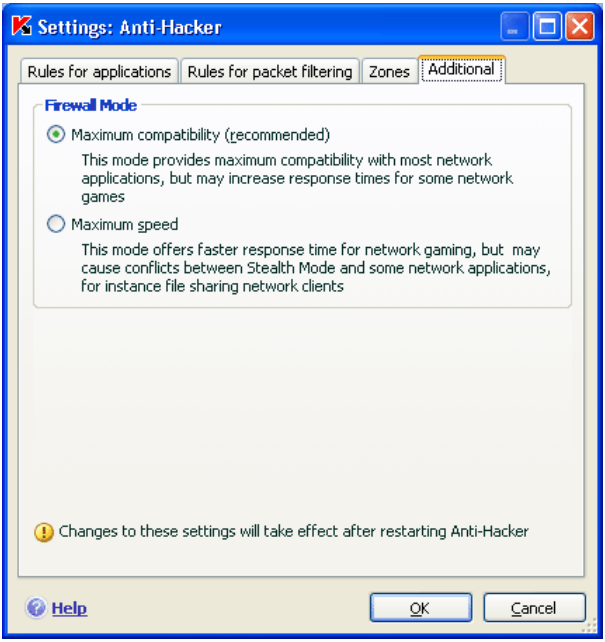

Settings: Anti-Hacker
Rules for applications
Rules for packet filtering
Zones
Additional
Firewall Mode
Maximum compatibility (recommended)
This mode provides maximum compatibility with most network applications, but may increase response times for some network games
Maximum speed
This mode offers faster response time for network gaming, but may cause conflicts between Stealth Mode and some network applications, for instance file sharing network clients
Changes to these settings will take effect after restarting Anti-Hacker
Help
OK
Cancel

Figure 49. Selecting an Anti-Hacker mode

Maximum compatibility – the Firewall ensures that Anti-Hacker will work optimally with programs that establish multiple network connections, for example, file-sharing network clients. However, this mode may lead to slow reaction time in network games. If you encounter such problems, you are advised to use Maximum Speed.

Maximum speed – the Firewall ensures the best possible reaction time during network games. However, file-sharing network clients and other network applications may experience conflicts with this mode. To solve the problem, disable Stealth Mode.

To select a Firewall mode:

1. Open the application settings window and select **Anti-Hacker** under **Protection**.
2. Click **Settings** in the Firewall section of the Anti-Hacker settings window.
3. Select the **Additional** tab in the window that opens and select the mode you want, Maximum Compatibility or Maximum Speed.

Changes to the Firewall settings will not take effect until after Anti-Hacker has been restarted.

12.8. Configuring the Intrusion Detection System

All currently known network attacks that could endanger the computer are listed in the threat signatures, and updated during signature updates. Kaspersky Anti-Virus does not update attack signatures by default (see 16.4.2 on pg. 211).

The Intrusion Detection System tracks network activity typical of network attacks and if it detects an attempt to attack your computer, it blocks all network activity between the remote computer and your computer for one hour. A warning will appear on the screen stating that a network attack attempt has taken place, with specific information about the computer which attacked you.

You can configure the Intrusion Detection System. To do so:

1. Open the application settings window and select **Anti-Hacker** under **Protection**.
2. Click **Settings** in the **Intrusion Detection System** section.
3. In the window that opens (see Figure 50), determine whether you want to block an attacking computer and, if so, for how long. The default blocked time is 60 minutes. You can increase or decrease the blocked time by changing the value in the field next to ☑ **Block the attacking computer for … min**. If you want to stop blocking traffic from an attacking computer directed at your computer, uncheck this box.

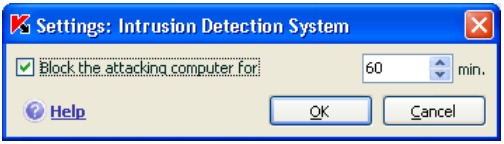


Figure 50. Configuring the block time for attacking computers

12.9. List of network attacks detected

There are currently a multitude of network attacks that utilize operating system vulnerabilities and other software, system or otherwise, installed on your computer. Malefactors are constantly perfecting attack methods, learning how to steal confidential information, making your system malfunction, or take over your computer to use it as part of a zombie network for carrying out new attacks.

To ensure your computer's security, you must know what kinds of network attacks you might encounter. Known network attacks can be divided into three major groups:

- **Port scan** – this threat is not an attack in its own right, but usually precedes one, since it is one of the common ways of obtaining information about a remote computer. The UDP/TCP ports used by the network programs are scanned to find out what state they are in (closed or open).

  Port scans can tell a hacker what types of attacks will work on the system, and what types will not. In addition, the information obtained by the scan will let the hacker determine what operating system the remote computer uses. This in turn further restricts the number of potential attacks, and, correspondingly, the time spent running them. It also aids a hacker in attempting to use vulnerabilities particular to that operating system.

- **DoS (Denial of Service) attacks** – these are attacks that render the attacked system unstable or entirely inoperable. These attacks can damage or corrupt the targeted information resources, and leave them unusable.

  There are two basic types of DoS attacks:

  - Sending the target computer specially created packets that the computer does not expect, which cause the system either to restart or to stop

- Sending the target computer many packets within a timeframe that the computer cannot process, which exhaust system resources

The following attacks are common examples of this type of attack:

- *Ping of death* sends an ICMP packet greater than the maximum of 64 KB. This attack can crash some operating systems.
- *Land* sends a request to an open port on your computer to establish a connection with itself. This sends the computer into a cycle, which intensifies the load on the processor and can end with some operating systems crashing.
- *ICMP Flood* sends a large number of ICMP packets to your computer. The attack leads to the computer being forced to reply to each inbound packet, which seriously weighs down the processor.
- *SYN Flood* sends a large number of queries to your computer to establish a fake connection. The system reserves certain resources for each of those connections, which completely drains your system resources, and the computer stops reacting to other connection attempts.

- **Intrusion attacks**, which aim to take over your computer. This is the most dangerous type of attack, since if it is successful, the hacker has complete control of your computer.

  Hackers use this attack to obtain confidential information from a remote computer (for example, credit card numbers or passwords), or to use its resources later for malicious purposes (e.g. using the captured system in zombie networks or as a platform for new attacks).

  This group contains more different types of attacks than any other. They can be divided into three subgroups based on operating system: Microsoft Windows attacks, Unix attacks, and a group for network services running either operating system.

  The most common types of attacks that use operating system network tools are:

  - *Buffer overflow attacks* – a type of software vulnerability that surfaces due to insufficient control in handling massive amounts of data. This is one of the oldest vulnerability types, and the easiest for hackers to exploit.
  - *Format string attacks* – a type of software vulnerability that arises from insufficient control of input values for I/O functions such as *printf()*, *fprintf()*, *scanf()*, and others from the C standard

library. If a program has this vulnerability, a hacker, using queries created with a special technique, can gain complete control of the system.

The Intrusion Detection System automatically analyzes and blocks attempts to exploit vulnerabilities in the most common network tools (FTP, POP3, IMAP) running on the user's computer.

Microsoft Windows attacks are based on taking advantage of vulnerabilities in software installed on the computer (for example, programs such as Microsoft SQL Server, Microsoft Internet Explorer, Messenger, and system components that can be accessed through the network – DCom, SMB, Wins, LSASS, IIS5).

Anti-Hacker protects your computer from attacks that use the following known software vulnerabilities (this list of vulnerabilities is cited with the Microsoft Knowledge Base numbering system):

(**MS03-026**) DCOM RPC Vulnerability(Lovesan worm)

(**MS03-043**) Microsoft Messenger Service Buffer Overrun

(**MS03-051**) Microsoft FrontPage 2000 Server Extensions Buffer Overflow

(**MS04-007**) Microsoft Windows ASN.1 Vulnerability

(**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow

(**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling

(**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

In addition, there are isolated incidents of intrusion attacks using various malicious scripts, including scripts processed by Microsoft Internet Explorer and Helkern-type worms. The essence of this attack type consists of sending a special type of UDP packets to a remote computer that can execute malicious code.

Remember that, while connected to the network, your computer is at constant risk of being attacked by a hacker. To ensure your computer's security, be sure to enable Anti-Hacker when using the Internet and regularly update hacker attack signatures (see 16.4.2 on pg. 211).

12.10. Blocking and allowing network activity

If the security level for the Firewall is set to **Training Mode**, a special notice appears on screen each time a network connection is attempted that has no rule.

For example, after opening Microsoft Outlook, it downloads your email from a remote Exchange server. To display your Inbox, the program connects to the email server. Anti-Hacker always tracks this kind of network activity. A message will appear on the screen (see Figure 51) containing:

- *Description of activity* – name of the application and a brief description of the connection that it is initiating, generally including the connection type, the local port from which it is being initiated, the remote port, and the address being connected to. Left click anywhere in the area to obtain detailed information on the connection, its initiating process, and the application distributor.
- *Action* – series of operations that Anti-Hacker will perform regarding the network activity detected.

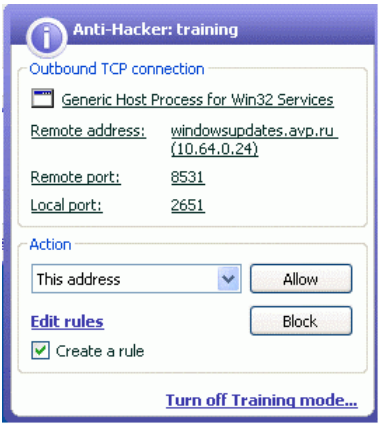


Figure 51. Network activity notification

Carefully review the information on network activity and only then select actions for Anti-Hacker. We recommend that you use these tips when making a decision:

1. Before doing anything else, decide whether to allow or block the network activity. It is possible that in this situation a set of rules already created for this application or packet will help you (assuming that such have been created). To do so, use the **Edit rules** link. Then a window

will open with a complete list of rules created for the application or data packet.

2. Decide whether to perform this action once or automatically every time this activity is detected.

To perform the action this time only:

uncheck **Create a rule** and click the button with the name of the action, e.g. **Allow**.

To perform the action you select automatically every time this activity is initiated on your computer:

1. Убедитесь, что флажок **Создать правило** установлен.
2. Select the type of activity that you want the action to apply to from the dropdown list in the **Action** section:
   - **All activity** – any network activity initiated by this application.
   - **Custom** – a single activity which you need to define in the rules dialog (see 12.2.1 on pg. 145).
   - **<Template>** – name of the template that includes the set of rules typical of the program's network activity. This activity type appears on the list if Kaspersky Anti-Virus for Windows Workstations includes an appropriate template for the application that initiated the network activity (see 12.2.2 on pg. 146). In such a case, you will not have to customize what activity to allow or block. Use the template and a set of rules for the application will be created automatically.
3. Click the button with the name of the action (**Allow** or **Block**).

Remember that the rule created will be used only when all of the connection parameters match it. This rule will not apply to a connection established from a different local port, for example.

To deactivate Anti-Hacker messages displayed for any application attempting to establish a network connection, click Disable Training Mode. This will place Anti-Hacker in the Allow All mode which allows all network connections except for those explicitly disallowed by rules.

CHAPTER 13. PROTECTION AGAINST UNWANTED E-MAIL

The Kaspersky Anti-Virus for Windows Workstations component which detects spam, processes it according to a set of rules, and saves you time when using email, is called *Anti-Spam*.

Anti-Spam uses the following method to determine whether an email is spam:

1. The sender's address is scanned for matches on black and white lists of addresses.
    - If the sender's address is on the white list, the email is marked as *accepted*.
    - If the sender's address is on the black list, the email is marked as *spam*. Further processing depends on the action you select (see 13.3.7 on pg. 180).
2. If the sender's address is not found on the white or black list, the email is analyzed using PDB technology (see 13.3.2 on pg. 171).
3. Anti-Spam examines the text of the email in detail and scans it for lines from the black or white list.
    - If the text of the email contains lines from the white list of lines, the email is marked as *accepted*.
    - If phrases from the phrase black list are encountered, the email is marked as *spam*. Further processing depends on the action you specify.
4. If the email does not contain phrases from the black or white list, it is analyzed for phishing. If the text of the email contains an address contained in the anti-phishing database, the email is marked as *spam*. Further processing depends on the action you specify.
5. If the email does not contain phishing lines, it is scanned for spam using special technologies:
    - Image analysis using GSG technology
    - Message text analysis using the iBayesian algorithm for spam recognition

6. Finally the email is scanned for advanced spam filtration factors (see 13.3.5 on pg. 177) specified by the user when Anti-Spam was installed. This could include scanning for correctness of HTML tags, font size, or hidden characters.

You can enable or disable each of these stages of the analysis.

Anti-Spam exists as a plug-in for the following email clients:

- Microsoft Outlook (see 13.3.8 on pg. 180)
- Microsoft Outlook Express (Windows Mail) (see 13.3.9 on pg. 183)
- The Bat! (see 13.3.10 on pg. 184)

This version of Kaspersky Anti-Virus does not support an Anti-Hacker plugin for Microsoft Office Outlook under Windows 98.

The task panel for Microsoft Outlook and Outlook Express (Windows Mail) clients has two buttons, **Spam** and **Not Spam**, which can configure Anti-Spam to detect spam right in your mailbox. In The Bat! there are no such buttons: instead the program can be trained using the special items **Mark as spam** and **Mark as NOT spam** on the **Special** menu. In addition, special processing parameters (see 13.3.1 on pg. 170) for spam are added to all the settings of the email client.

Anti-Spam uses special self-training iBayes algorithm, which allows the component over time to more accurately distinguish between *spam* and *accepted email*. The data source for the algorithm is email contents.

Situations arise when iBayes is unable to classify a certain email as either spam or accepted email to a high degree of accuracy. These emails are marked as *potential spam*.

In order to reduce the number of emails marked as potential spam, you are advised to conduct additional Anti-Spam training (see 13.2 on pg. 166) on such emails. To do so, you must specify which of those emails should be marked as *spam*, and which as *accepted*.

Emails that are *spam* or *potential spam* are modified: the markings **[!! SPAM]** or **[?? Probable Spam]**, are added to the subject line.

The rules for processing spam or potential spam emails for Microsoft Outlook, Microsoft Outlook Express (Windows Mail), or The Bat! are specified in special plug-in components within the email client itself. For other email clients, you can configure filtration rules that search for the modified subject line containing **[!! SPAM]** or **[?? Probable Spam]** and move the email to a designated folder. For more information about the filtration mechanism, please consult the documentation for your email client.

13.1. Selecting an Anti-Spam sensitivity level

Kaspersky Anti-Virus for Windows Workstations protects you from spam at one of the following levels (see Figure 52):

Block all – strictest level of sensitivity, at which only messages containing phrases from the phrase white list (see 13.3.4.1 on pg. 174) and senders listed on the white list are accepted: everything else is marked as spam. At this level, email is only analyzed against the white lists. All other features all disabled.

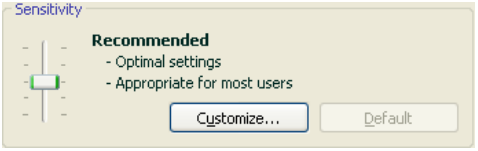


Figure 52. Selecting the Anti-Spam security level

High – a strict level that when activated raises the likelihood that some emails that are not spam will be marked as *spam*. At this level, email is analyzed against the white and black lists, and also using PDB and GSG technologies, and iBayes algorithm (see 13.3.2 on pg. 171).

This level should be applied in cases when there is a high likelihood that the recipient's address is unknown to spammers. For example, when the recipient is not signed to mass mailings, and does not have an email address on free/non-corporate email servers.

Recommended – the standard universal settings level for classifying email.

At this level, it is possible that some spam will not be detected. This shows that Anti-Spam is not trained well enough. You are advised to conduct additional training for the module using the Training Wizard (see 13.2.1 on pg. 167) or the **Spam**/**NOT Spam** buttons (or corresponding menu items in The Bat!) for emails that were incorrectly marked.

Low – the most flexible settings level. It is recommended for users whose incoming correspondence contains a significant number of words recognized by Anti-Spam as spam, but is not spam. This may be because of the recipient's professional activity, which forces him to use professional terms in his correspondence with colleagues that are widespread in spam. All spam detection technologies are used to analyze emails at this level.

Skip all – lowest sensitivity level. Only email that contains phrases from the phrase black list, or senders listed on the address black list, are marked as

spam. At this level, email is only processed using the black list, and all other features all disabled.

By default, Anti-Spam is set to the **Recommended** sensitivity level. You can boost or reduce the level or edit the settings for the current level.

To modify the level of protection:

In the Sensitivity section, move the slider up or down to the required setting. By adjusting the sensitivity level, you define the correlation between spam, potential spam, and accepted email factors (see 13.3.3 on pg. 172).

To modify the settings for the current level:

In the application's Settings window, click on **Anti-Spam** to show the components settings. Click the **Customize** button in the Sensitivity section. Edit the spam factor in the window that opens and click **OK**.

The security level's name will then change to **Custom**.

13.2. Training Anti-Spam

Anti-Spam comes with a pre-installed email database containing fifty spam samples. You are advised to give the Anti-Spam module further training on your own emails.

There are several approaches to training Anti-Spam:

- Use the Training Wizard (see 13.2.1 on pg. 167)
- Train Anti-Spam with outgoing emails (see 13.2.2 on pg. 167)
- Train directly while working with email (see 13.2.3 on pg. 168), using special buttons in the email client tools panel or menu items
- Training in Anti-Spam reports (see 13.2.4 on pg. 168)

The best method is to use the Training Wizard from the very onset of using Anti-Spam, as it can train Anti-Spam on a large number of emails.

Note that you cannot train Anti-Spam with more than 50 emails per folder. If there are more emails in the folder, the program will use fifty for training.

Additional training, using special buttons in the email client interface, are preferable when working directly with email.

13.2.1. Training Wizard

The Training Wizard trains Anti-Spam by indicating which mailbox folders contain spam and which contain accepted email.

To open the Training Wizard:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Click the **Training Wizard** button Training section of the settings window.

Training Wizard includes step-by-step procedures for training Anti-Spam. Use the **Back** and **Next** buttons to navigate between steps.

Step One of the Training Wizard involves selecting folders that contain accepted email. At this stage, you must only select the folders whose contents you fully trust.

Step Two of the Training Wizard consists of selecting folders that contain spam. Skip this step if your mail client does not have spam folders.

In Step Three, Anti-Spam is automatically trained on the folders you selected. The emails in those folders populate the Anti-Spam database. The senders of accepted email are automatically added to the address white list.

In Step Four, the results of training must be saved using one of the following methods: add the results of training to the current Anti-Spam database or replace the current database with the results of training. Please bear in mind that the program must be trained on at least 50 accepted emails and 50 junk emails for iBayes to work accurately.

To save time, the Training Wizard only trains on 50 emails in each selected folder.

13.2.2. Training with outgoing emails

You can train Anti-Spam with outgoing emails from your email client. Then the Anti-Spam address white list will be filled by analyzing outgoing messages. Only the first fifty emails are used for training, at which point, training is complete.

To train Anti-Spam with outgoing emails:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Check **Train with outgoing emails** in the **Training** section.

Warning!

Anti-Spam will only train itself with outgoing emails sent via MAPI protocol if you check **Scan upon sending** in the Microsoft Outlook Mail Anti-Virus plug-in (see 13.3.8 on pg. 180).

13.2.3. Training using your email client

To training while using your mailbox, you use special buttons on your email client's tools panel.

When you install Anti-Spam on your computer, it installs plug-ins for the following email clients:

- Microsoft Outlook
- Outlook Express (Windows Mail)
- The Bat!

For example, the task panel of Outlook has two buttons, **Spam** and **Not Spam,** and a **Kaspersky Anti-Spam** tab of settings (see 13.3.8 on pg. 180) in the Options dialog box (menu item **Service→ Options**). Outlook Express, in addition to the **Spam** and **Not Spam** buttons, adds a **Configure** button to the task panel that opens a window with actions (see 13.3.9 on pg. 183) when spam is detected. In The Bat! there are no such buttons, although the program can be trained using the special items **Mark as spam** and **Mark as NOT spam** on the **Special** menu.

If you decide that the currently open email is spam, click the **Spam** button. If the email is not spam, click **Not Spam**. After this, Anti-Spam will training itself using the email. If you select several emails, all of them will be used for training.

Warning!

In cases when you need to immediately select several emails, or are certain that a certain folder only contains emails of one group (spam or not spam), you can take a comprehensive approach to training using the Training Wizard (see 13.2.1 on pg. 167).

13.2.4. Training using Anti-Spam reports

You have the option of training Anti-Spam through its reports.

To view the component's reports:

1. Select **Anti-Spam** component in the **Protection** section of the main program window.
2. Left-click in the **Statistics** box (see Figure 53).

The component's reports can help you make a conclusion about the accuracy of its configuration, and, if necessary, make certain corrections to Anti-Spam.

To mark a certain email as spam or not spam:

1. Select it from the report list on the **Events** tab, and use the **Actions** button.
2. Select one of the four options:
   - **Mark as Spam**
   - **Mark as Not Spam**
   - **Add to White list**
   - **Add to Black list**

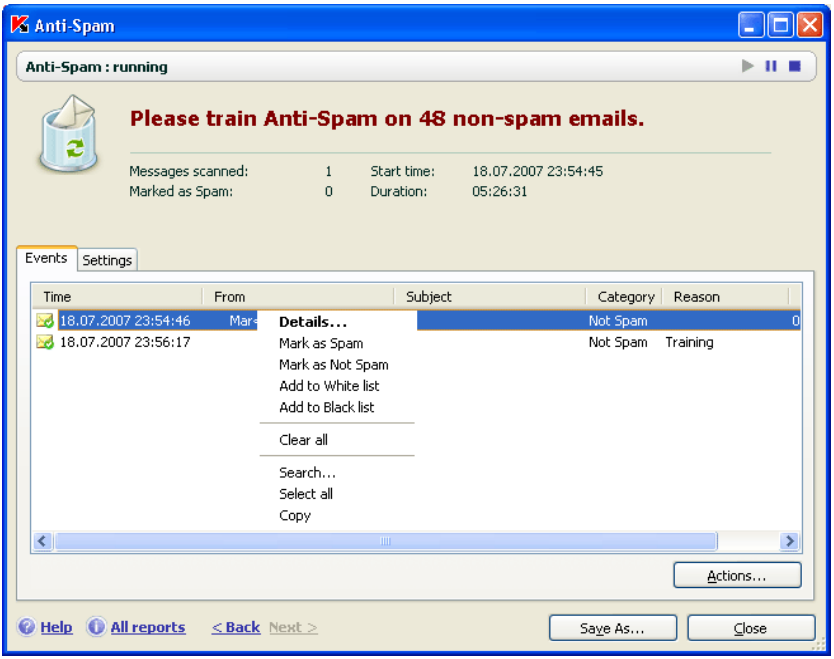


Figure 53. Training Anti-Spam from reports

Anti-Spam will continue further training based on this email.

13.3. Configuring Anti-Spam

Fine-tuning Anti-Spam is essential for the spam security feature. All settings for component operation are located in the Kaspersky Anti-Virus for Windows Workstations settings window and allow you to:

- Determine the particulars of operation of Anti-Spam (see 13.3.1 on pg. 170)
- Choose which spam filtration technologies to use (see 13.3.2 on pg. 171)
- Regulate the recognition accuracy of spam and potential spam (see 13.3.3 on pg. 172)
- Create white and black lists for senders and key phrases (see 13.3.4 on pg. 173)
- Configure additional spam filtration features (see 13.3.5 on pg. 177)
- Maximally reduce the amount of spam in your Inbox through previewing with the Email Dispatcher (see 13.3.6 on pg. 179)

The following sections will examine these settings in detail.

13.3.1. Configuring scan settings

You can configure the following scan settings:

- Whether traffic from POP3/IMAP protocols are scanned. By default, Kaspersky Anti-Virus scans email on all these protocols.
- Whether plug-ins are activated for Outlook, Outlook Express (Windows Mail), and The Bat!
- Whether email is viewed via POP3 in the Email Dispatcher (see 13.3.6 on pg. 179) prior to downloading it from the email server to the user's Inbox.

To configure these settings:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Check or uncheck the boxes in the Connectivity section which correspond to the three options discussed immediately above (see Figure 54).
3. Edit the network settings, if necessary.

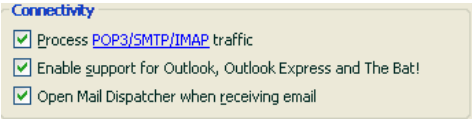

Connectivity
Process POP3/SMTP/IMAP traffic
Enable support for Outlook, Outlook Express and The Bat!
Open Mail Dispatcher when receiving email

Figure 54. Configuring scan settings

Warning!

If you use Microsoft Outlook Express you should restart it when changing status of Enable support for Outlook, Outlook Express and The Bat! flag.

13.3.2. Selecting spam filtration technologies

Emails are scanned for spam using state-of-the-art filtration technologies:

- **iBayes**, based on the Bayes theorem, analyzes email text to detect phrases that mark it as spam. The analysis uses the statistics obtained by training Anti-Spam (see 13.2 on pg. 166).
- **GSG**, which analyzes graphic elements in emails using special graphic signatures to detect spam in graphics.
- **PDB**, which analyzes email headers and classifies them as spam based on a set of heuristic rules.

By default, all of these filtration technologies are enabled, checking email for spam as completely as possible.

To disable any of these filtration technologies:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Click on the **Customize** button in the **Sensitivity** section, and in the window that opens select the **Spam Recognition** tab (see Figure 55).
3. Uncheck the boxes next to the filtration technologies that you do not want to use for detecting spam.

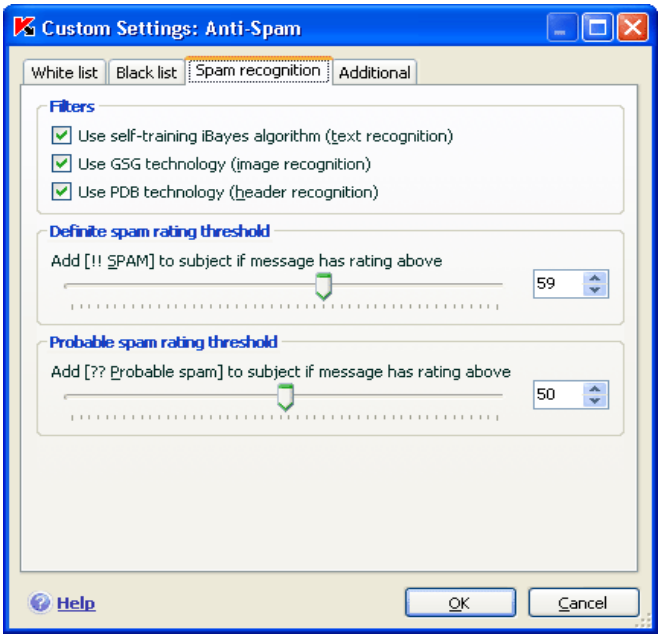


Figure 55. Configuring spam recognition

13.3.3. Defining spam and potential spam factors

Kaspersky Lab specialists have optimally configured Anti-Spam to recognize spam and probable spam.

Spam detection operates on state-of-the-art filtration technologies (see 13.3.2 on pg. 171), and on training Anti-Spam to recognize spam, potential spam, and accepted email accurately using emails from your Inbox.

Anti-Spam is trained using the Training Wizard, and through email client programs. During training, every individual element of accepted emails or spam is assigned a factor. When an email enters your inbox, Anti-Spam scans the email with iBayes for elements of spam and of accepted email. The factors for each element are totaled and the email is given a *spam factor* and an *accepted email factor*.

The probable spam factor defines the likelihood that the email will be classified as probable spam. If you are using the **Recommended** level, any email has

between a 50% and 59% chance of being considered *probable spam*. Good mail refers to mail that, after being scanned, has a spam factor of less than 50%.

The spam factor determines the likelihood that Anti-Spam will classify an email as spam. Any email with chances beyond that indicated above will be perceived as spam. The default spam factor is 59% for the **Recommended** level. This means that any email with a likelihood of more than 59% will be marked as *spam*.

In all, there are five sensitivity levels (see 13.1 on pg. 165), three of which (**High, Recommended**, and **Low**) are based on various spam and probable spam factor values.

You can edit the Anti-Spam algorithm on your own. To do so:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. In the **Sensitivity level** box on the right-hand side of the window, click **Customize**.
3. In the window that opens, adjust the spam and probable spam factors in the sections for them on the **Spam Recognition** tab (see Figure 55).

13.3.4. Creating white and black lists manually

Users can create black and white lists manually, by using Anti-Spam with their email. These lists store information on user addresses that are considered safe or spam sources, and various key words and phrases that identify them as spam or accepted email.

The chief application of the lists of key phrases, and in particular the white list, is that you can coordinate with trusted addressees, (for example, with colleagues), signatures containing a particular phrase. You could use, for example, a PGP signature as an email signature. You can use wildcards in the signatures and in the addresses: * and ?. A * represents any sequence of characters of any length. A question mark represents any one character.

If there are asterisks and questions marks in the signature, to prevent errors with Anti-Spam processes them, they should be preceded by a backslash. Then two characters are used instead of one: * and \?.

13.3.4.1. White lists for addresses and phrases

The white list contains key phrases from emails that you marked as *accepted*, and addresses of trusted senders who would not send spam. The white list is filled manually, and the list of senders' addresses is done automatically while training the Anti-Spam component. You can edit this list.

To configure the white list:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Click the **Settings** button in the right-hand part of the settings window.
3. Open the **White list** tab (see Figure 56).

The tab is divided into two sections: the upper portion contains the addresses of senders of good email, and the lower contains key phrases from such emails.

To enable phrase and address white lists during spam filtration, check the corresponding boxes in the **Allowed senders** and **Allowed phrases** sections.

You can edit the lists using the buttons in each section.

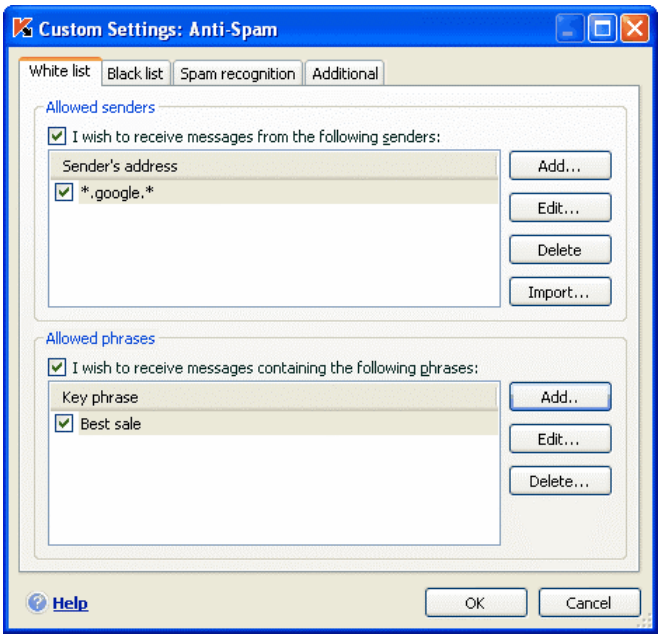


Figure 56. Configuring address and phrase white lists

You can assign both addresses and address masks in the address list. When entering an address, the use of capitals is ignored. Let's look at some examples of address masks:

- *ivanov@test.ru* – emails from this address will always be classified as accepted.
- **@test.ru* – email from any sender in the domain *test.ru* is accepted, for example: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – a sender with this name, regardless of the email domain, always sends only accepted email, for example: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – email from any sender in a domain that begins with *test* is not spam, for example: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – email from a sender whose name begins with ivan. and whose domain name begins with *test* and ends in any three characters is always accepted, for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

You can also use masks for phrases. When entering a phrase, the use of capitals is ignored. Here are some examples of some of them:

- *Hi, Ivan!* – an email that only contains this text is accepted. It is not recommended to use such a phrase as a white list phrase.
- *Hi, Ivan!** – an email beginning with the phrase *Hi, Ivan!* is accepted.
- *Hi, *! ** – emails beginning with the greeting *Hi* and an exclamation point anywhere in the email will not to be treated as spam.
- ** Ivan? ** – the email contains a greeting to a user with the name *Ivan*, whose name is followed by any character, and is not spam.
- ** Ivan\? ** – emails containing the phrase *Ivan?* are accepted.

To disable the use of a certain address or phrase as attributes of good email, it can be deleted using the Delete button, or the box alongside the text can be unchecked to disable them.

You have the option of importing CSV-formatted files for white list addresses.

13.3.4.2. Black lists for addresses and phrases

The sender black list stores key phrases from emails that constitute *spam*, and the addresses of their senders. The list is filled manually.

To fill the black list:

1. Select **Anti-Spam** in the Kaspersky Anti-Virus for Windows Workstations settings window.
2. Click the **Settings** button in the right-hand part of the settings window.
3. Open the **Black list** tab (see Figure 57).

The tab is divided into two sections: the upper portion contains the addresses of spam senders, and the lower contains key phrases from such emails.

To enable phrase and address black lists during spam filtration, check the corresponding boxes in the **Blocked senders** and **Blocked phrases** sections.

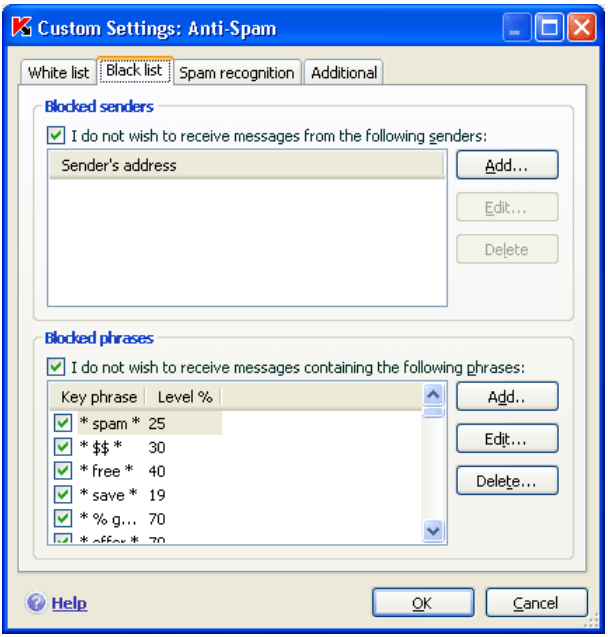


Figure 57. Configuring address and phrase black lists

You can edit the lists using the buttons in each section.

You can assign both addresses and address masks in the address list. When entering an address, the use of capitals is ignored. Let's look at some examples of address masks:

- *ivanov@test.ru* – emails from this address will always be classified as accepted.

- **@test.ru* – email from any sender in the domain *test.ru* is accepted, for example: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – a sender with this name, regardless of the email domain, always sends only accepted email, for example: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – email from any sender in a domain that begins with *test* is not spam, for example: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – email from a sender whose name begins with ivan. and whose domain name begins with *test* and ends in any three characters is always accepted, for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

You can also use masks for phrases. When entering a phrase, the use of capitals is ignored. Here are some examples of some of them:

- *Hi, Ivan!* – an email that only contains this text is accepted. It is not recommended to use such a phrase as a white list phrase.
- *Hi, Ivan!** – an email beginning with the phrase *Hi, Ivan!* is accepted.
- *Hi, *! ** – emails beginning with the greeting *Hi* and an exclamation point anywhere in the email will not to be treated as spam.
- ** Ivan? ** – the email contains a greeting to a user with the name *Ivan*, whose name is followed by any character, and is not spam.
- ** Ivan\? ** – emails containing the phrase *Ivan?* are accepted.

To disable the use of a certain address or phrase as attributes of spam, it can be deleted using the Delete button, or the box alongside the text can be unchecked to disable them.

13.3.5. Additional spam filtration features

In addition to the main features that are used to filter spam (creating white and black lists, phishing analysis, filtration technologies), Kaspersky Anti-Virus for Windows Workstations provides you with advanced features.

To configure advanced spam filtration features:

1. Open the application settings window and select **Anti-Spam** under **Protection**.
2. Click the **Customize** button in the Sensitivity section of the settings window.
3. Open the **Additional** tab (see Figure 58).

The tab lists a series of indicators that will classify email as being, more likely than not, spam.

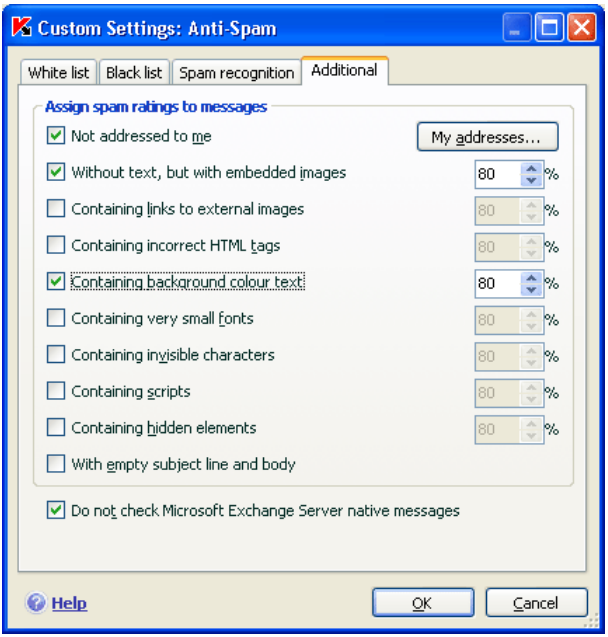


Figure 58. Advanced spam recognition settings

To use an additional filtration indicator, check the flag beside it. Each of the factors also requires that you set a spam factor (in percentage points) that defines the likelihood that an email will be classified as spam. The default value for the spam factor is 80%. The email will be marked as spam if the sum of the likelihoods for all additional factors exceeds 100%.

Spam could be empty e-mails (no subject or body), e-mails containing links to images or with imbedded images, with text that matches the background color, or text in a very small font size. Spam can also be e-mails with invisible characters (the text matches the background color), e-mails containing hidden elements (the elements are not displayed at all), or incorrect html tags, as well as e-mails containing scripts (a series of instructions executed when the user opens the e-mail).

If you activate a filter to capture “messages not addressed to me”, you will need to create a list of trusted addresses accessible through the **My Addresses** button. The recipient’s address will be scanned when the e-mail is analyzed. If the address does not match any of those on your list, the e-mail will be labeled as *spam*.

You can create and edit an address list in the **My addresses** using the **Add**, **Edit**, and **Delete** button.

To exclude e-mails forwarded within the intranet (for example, corporate e-mail) from the spam scan, check **Do not scan internal Microsoft Exchange Server** mail. Note that e-mails will be considered internal mail if all the computers on the network use Microsoft Office Outlook as their mail client, and if the user e-mail boxes are located on one Exchange server, or these servers must be connected with X400 connectors. For Anti-Spam to analyze these e-mails, deselect the checkbox.

13.3.6. Mail Dispatcher

> Warning!
> Mail Dispatcher is only available if you receive email via POP3 protocol.

Mail Dispatcher is designed for viewing the list of email messages on the server without downloading them to your computer. This enables you to refuse to accept messages, saving time and money when working with email and reducing the likelihood of downloading spam and viruses to your computer.

Mail Dispatcher opens if the **Anti-Spam** settings window **Open Mail Dispatcher when receiving email** is checked in the Anti-Spam settings.

To delete emails from the server without downloading them onto your computer:

check the boxes on the left of the emails that you want to delete, and click the **Delete** button. The emails checked with be deleted from the server. The rest of your email will be downloaded to your computer after you close the Mail Dispatcher window.

Sometimes it can be difficult to decide whether to accept a certain email, judging only by the sender and the email's subject line. In such cases, Mail Dispatcher gives you more information by downloading the email's headers.

To view email headers:

select the email from the list of incoming email. The email's headers will be displayed in the lower part of the form.

Email headers are not of a significant size, generally a few dozen bytes, and cannot contain malicious code.

Here is an example of when it might help to view an email's headers: spammers have installed a malicious program on a coworker's computer that sends spam with his name on it, to everyone on his email client's contact list. The likelihood that you are on your coworker's contact list is extremely high, and undoubtedly your inbox will become full of spam from him. It is impossible to tell, judging by

the sender's address alone, whether the email was sent by your coworker or a spammer. The email headers will however reveal this information, allowing you to check who sent the email, when, and what size it is, and to trace the email's path from the sender to your email server. All this information should be in the email headers. You can then decide whether it is really necessary to download that email from the server, or if it is better to delete it.

Note:

You can sort emails by any of the columns of the email list. To sort, click on the column heading. The rows will be sorted in ascending order. To change the sorting direction, click on the column heading again.

13.3.7. Actions for spam

If after scanning you find that an email is spam or potential spam, the next steps that Anti-Spam takes depend on the object status and the action selected. By default, emails that are *spam* or *potential spam* are modified: the markings **[!! SPAM]** or **[?? Probable Spam]** are added to the subject line.

You can select additional actions for spam or potential spam. In Microsoft Outlook, Outlook Express (Windows Mail) and The Bat! special plug-ins are provided to do so. For other email clients, you can configure the filtration rules.

13.3.8. Configuring spam processing in Microsoft Office Outlook

Note that there is no spam plug-in for Microsoft Outlook if you are running the application under Windows 9x.

Email that is classified by Anti-Spam as *spam* or *potential spam* is by default marked with special markings **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** line.

Additional actions for spam and potential spam in Outlook can be found on the special **Anti-Spam** tab on the **Service→ Options** menu (see Figure 59).

It opens automatically when the email client is first opened after installing the program and asks if you to configure spam processing.

You can assign the following processing rules for both spam and potential spam:

Move to folder – spam is moved to the specified folder.

Copy to folder – a copy is created of the email and it is moved to the specified folder. The original email stays in your Inbox.

Delete – deletes spam from the user's mailbox.

Skip – leaves the email in your Inbox.

To do so, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

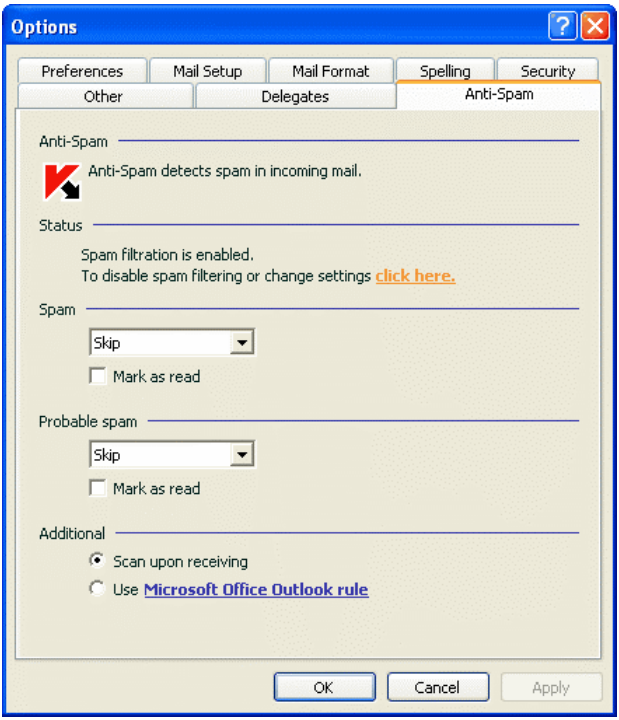


Figure 59. Configuring spam processing in Microsoft Office Outlook

You can also configure Microsoft Office Outlook and Anti-Spam to work together:

Scan upon receiving. All emails that enter the user's inbox are initially processed according to the Outlook rules. After processing is complete, the Anti-Spam plug-in processes the remaining messages that do not fall under any of the rules. In other words, emails are processed according to the priority of the rules. Sometimes the priority sequence may be ignored, if, for example, a large number of emails arrive in your Inbox at the same time. In such a case, situations could arise when information about an email processed by an Outlook rule is logged in the Anti-Spam report as *spam*. To

avoid this, we recommend configuring the Anti-Spam plug-in as an Outlook rule.

Use Microsoft Office Outlook rule. With this option, incoming messages are processed based on a hierarchy of the Outlook rules created. One of the rules must be a rule about Anti-Spam processing emails. This is the best configuration. It will not cause conflicts between Outlook and the Anti-Spam plug-in. The only drawback to this arrangement is that you must create and delete spam processing rules through Outlook manually.

The Anti-Spam plug-in cannot be used as an Outlook rule in Microsoft Office XP if you are running 9x/ME/NT4 due to an error in Outlook XP.

To create a spam processing rule:

1. Open Microsoft Office Outlook and go to **Service →Rules and Alerts** in the main menu. The command for opening the Wizard depends on your version of Microsoft Office Outlook. This User Guide describes how to create a rule using Microsoft Office Outlook 2003.
2. In the **Rules and Alerts** windows that opens, click **New Rule** on the **E-mail Rules** tab to open the Rules Wizard. The **Rule Wizard** will guide you through the following windows and steps:

   Step One

   You can choose to create a rule from scratch or from a template. Select **Start from a blank rule** and select **Check messages when they arrive**. Click the **Next** button.

   Step Two

   In the **Rule Conditions** window, click **Next** without checking any boxes. Confirm in the dialog box that you want to apply this rule to all emails received.

   Step Three

   In the window for selecting actions to apply to messages, check **perform a custom action** from action list. In the lower portion of the window click custom action. In the window that opens, select **Kaspersky Anti-Spam** from the dropdown menu and click **OK**.

   Step Four

   In the window for selecting exceptions to the rule, click **Next** without checking any boxes.

   Step Five

In the window for finishing creating the rule, you can edit its name (the default is **Kaspersky Anti-Spam**). Make sure that **Turn on this rule** is checked and click **Finish**.

3. The default position for the new rule is first on the rule list in the **E-mail Rules** window. If you like, move this rule to the end of the list so it is applied to the email last.

All incoming emails are processed with these rules. The order in which the rules are applied depends on their priority, with rules at the top of the list having higher priority than those lower down. You can change the priority for applying rules to emails.

If you do not want the Anti-Spam rule to further process emails after a rule is applied, you must check **Stop processing more rules** in the rule settings (see Step Three in creating a rule).

If you are experienced in creating email processing rules in Outlook, you can create your own rule for Anti-Spam based on the setup that we have suggested.

13.3.9. Configuring spam processing in Outlook Express (Windows Mail)

Email that is classified by Anti-Spam as *spam* or *potential spam* is by default marked with special markings **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** line.

Additional actions for spam and potential spam in Outlook Express (Windows Mail) can be found in the settings window that opens (see Figure 60) when you click the **Configure** button near the **Spam** and **Not Spam** buttons on the tasks panel.

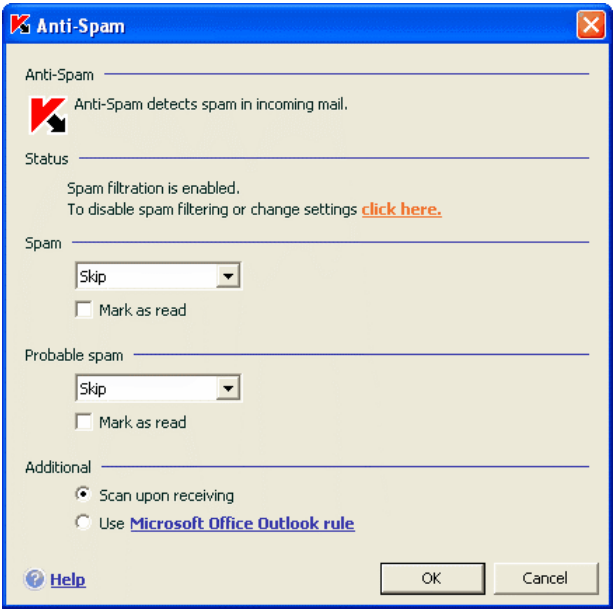


Figure 60. Configuring spam processing in Microsoft Outlook Express

It opens automatically when you first open the email client after installing the program, and asks if you want to configure spam processing.

You can assign the following processing rules for both spam and potential spam:

Move to folder – spam is moved to the specified folder.

Copy to folder – a copy is created of the email and it is moved to the specified folder. The original email stays in your Inbox.

Delete – deletes spam from the user's mailbox.

Skip – leaves the email in your Inbox.

To assign these rules, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

13.3.10. Configuring spam processing in The Bat!

Mail client should be restarted after enabling/disablig plugin for Microsoft Outlook Express.

Actions for spam and probable spam in The Bat! are defined by the email client's own tools.

To set up spam processing rules in The Bat!:

1. Select **Settings** from the email client's **Properties** menu.
2. Select **Anti-Spam** from the settings tree (see Figure 61).

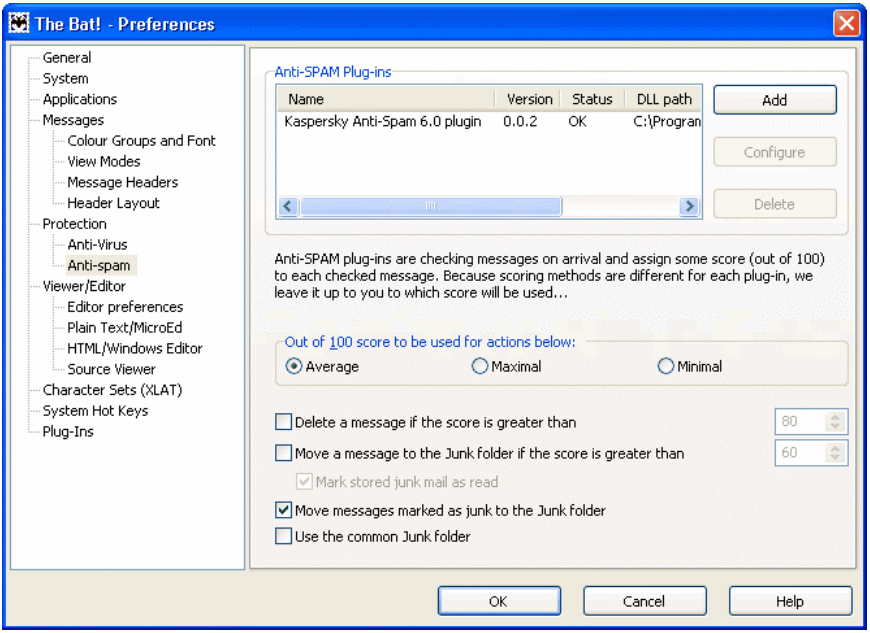


Figure 61. configuring spam recognition and processing in The Bat!

The protection settings for spam presented extend to all anti-spam modules installed on the computer that support work with The Bat!

You must set the rating level and specify how to respond to emails with a certain rating (in the case of Anti-Spam, the likelihood that the email is spam):

- Delete the emails with a rating higher than a given value.
- Move emails with a given range of ratings to a special folder for spam.
- Move spam marked with special headers to the spam folder.
- Leave spam in your Inbox.

Warning!

After processing an email, Kaspersky Anti-Virus for Windows Workstations assigns a spam or potential spam status to the email based on a factor (see 13.3.3 on pg. 172) with a value that you can adjust. The Bat! has its own spam rating method, also based on a spam factor. To ensure that there is no discrepancy between the spam factor in Kaspersky Anti-Virus for Windows Workstations and in The Bat!, all the emails scanned by Anti-Spam are assigned a rating in accordance with the email status categories used by The Bat!: *accepted email* – 0%, *probably spam – 50 %*, spam – *100 %*.

This way, the spam rating in The Bat! corresponds not to the email factor assigned in Anti-Spam but to the factor of the corresponding status.

For more details on the spam rating and processing rules, see documentation for The Bat!

CHAPTER 14. SCANNING FOR VIRUSES ON THE COMPUTER

One of the important aspects of protecting your computer is scanning user-defined areas for viruses. Kaspersky Anti-Virus for Windows Workstations can scan individual items – files, folders, disks, plug-and-play devices – or the entire computer. Scanning for viruses stops malicious code which has gone undetected by protection components from spreading.

Kaspersky Anti-Virus for Windows Workstations includes the following default scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses, including: system memory, programs loaded on startup, boot sectors on the hard drive, and the *Windows* and *system32* system directories. The task aims to detect active viruses quickly on the system without fully scanning the computer.

My Computer

Scans for viruses on your computer with a thorough inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses all programs loaded when the operating system boots.

The default settings for these tasks are the recommended ones. You can edit these settings (see 14.4.4 on pg. 196) or create a schedule (see 6.5 on pg. 82) for running tasks.

You also have the option of creating your own tasks (see 14.4.3 on pg. 195) and creating a schedule for them. For example, you can schedule a scan task for email databases once per week, or a virus scan task for the **My Documents** folder.

In addition, you can scan any object for viruses (for example, the hard drive where programs and games are, e-mail databases that you've brought home from work, an archive attached to an e-mail, etc.) without creating a special scan task. You can select an object to scan from the Kaspersky Anti-Virus for Windows Workstations interface, or with the standard tools of the Windows operating system (for example, in the **Explorer** program window or on your **Desktop**).

You can view a complete list of virus scan tasks for your computer by clicking on **Scan** in the left-hand pane of the main application window.

14.1. Managing virus scan tasks

You can run a virus scan task manually or automatically using a schedule (see 6.5 on pg. 82).

To start a virus scan task manually:

Check the box beside the task name in the **Scan** section of the main program window, and click the button on the status bar.

The tasks currently being performed (including tasks created through Kaspersky Administration Kit) are displayed in the context menu by right-clicking on the system tray icon

To pause a scan task:

Click the button on the status bar. The task status will change to *paused*. This will pause the scan until you start the task again manually or it starts again automatically according to the schedule.

To stop a scan task:

Click the button on the status bar. The task status will change to *stopped*. This will stop the scan until you start the task again manually or it starts again automatically according to the schedule. The next time you run the task, the program will ask if you would like to continue the task where it stopped or begin it over.

14.2. Creating a list of objects to scan

To view a list of objects to be scanned for a particular task, select the task name (for example, **My computer**) in the **Scan** section of main program window. The list of objects will be displayed in the right-hand part of the window under the status bar (see Figure 62).

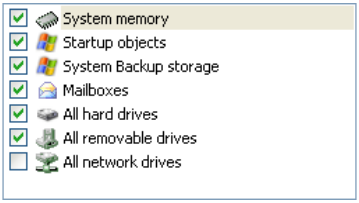


Figure 62. List of objects to scan

Object scan lists are already made for default tasks created when you install the program. When you create your own tasks or select an object for a virus scan task, you can create a list of objects.

You can add to or edit an object scan list using the buttons to the right of the list. To add a new scan object to the list, click the **Add** button, and in the window that opens select the object to be scanned.

For the user's convenience, you can add categories to a scan area such as user mailboxes, RAM, startup objects, operating system backup, and files in the Kaspersky Anti-Virus Quarantine folder.

In addition, when you add a folder that contains embedded objects to a scan area, you can edit the recursion by selecting an item in the scan list, opening a shortcut menu, and using the **Include Subfolders** option.

To delete an object, select it from the list (when you do so, the name of the object will be highlighted in gray) and click the **Delete** button. You can temporarily disable scanning for individual objects for any task without deleting them from the list. To do so, uncheck the box beside the object that you do not want scanned.

To start a scan task, click the **Scan** button, or select **Start** from the menu that opens when you click the **Actions** button.

In addition, you can select an object to be scanned with the standard tools of the Windows operating system (for example, in the Explorer program window or on your Desktop, etc.) (see Figure 63). To do so, select the object, open the Windows context menu by right-clicking, and select **Scan for Viruses**.

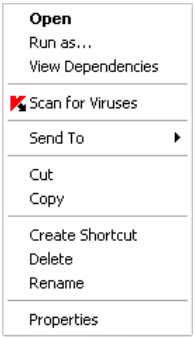


Figure 63. Scanning objects from the Windows context menu

14.3. Creating virus scan tasks

To scan objects on your computer for viruses, you can use built-in scan tasks included with the program and create your own tasks. New scan tasks are created using existing tasks that a template.

To create a new virus scan task:

1. Select the task with the settings closest to those you need, in the **Scan** section of the main program window.
2. Open the context menu by right-clicking on the task name, or click the **Actions** button to the right of the scan object list, and select **Save as...**.
3. Enter the name for the new task in the window that opens and click **OK**. A task with that name will then appear in the list of tasks in the **Scan** section of the main program window.

Warning!

There is a limit to the number of tasks that the user can create. The maximum is four tasks.

The new task is a copy of the one it was based on. You need to continue setting it up by creating an scan object list (see 14.2 on pg. 188), setting up properties that govern the task (see 14.4 on pg. 191), and, if necessary, configuring a schedule (see 6.5 on pg. 82) for running the task automatically.

To rename a created task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will also be changed in the **Scan** section.

To delete a created task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Delete**.

You will be asked to confirm that that you want to delete the task. The task will then be deleted from the list of tasks in the **Scan** section.

Warning!

You can only rename and delete tasks that you have created.

14.4. Configuring virus scan tasks

The methods are used to scan objects on your computer are determined by the properties assigned for each task.

To configure task settings:

open the application settings window and select a task by name under **Scan**.

You can use the settings window for each task to:

- Select the security level that the task will use (see 14.4.1 on pg. 192)
- Edit advanced settings:
    - define what file types are to be scanned for viruses (see 14.4.2 on pg. 193)
    - configure task start using a different user profile (see 6.4 on pg. 81)
    - configure advanced scan settings (see 14.4.5 on pg. 198)
- restore default scan settings (see 14.4.3 on pg. 195)
- select an action that the program will apply when it detects an infected or suspicious object (see 14.4.4 on pg. 196)
- create a schedule (see 6.5 on pg. 82) to automatically run tasks.
- In addition, you can configure global settings (see 14.4.6 on pg. 199) for running all tasks.

The following sections examine the task settings listed above in detail.

14.4.1. Selecting a security level

Each virus scan task can be assigned a security level (see Figure 64):

High – the most complete scan of the entire computer or individual disks, folders, or files. You are advised to use this level if you suspect that a virus has infected your computer.

Recommended – Kaspersky Lab experts recommend this level. The same files will be scanned as for the **High** setting, except for email databases.

Low – level with settings that let you comfortably use resource-intensive applications, since the scope of files scanned is reduced.

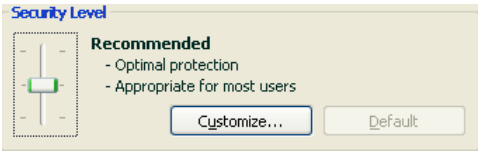


Figure 64. Selecting a virus scan security level

By default, file scanning level is set to **Recommended**.

You can raise or lower the scan security level by selecting the level you want or changing the settings for the current level.

To edit the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the file security levels listed meet your needs, you can customize the scan settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. If you do so, the level will be renamed as **Custom**.

To modify the settings for a security level:

click the **Settings** button in the task settings window. Edit the scan settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom settings**, which contains the scan settings that you configured.

14.4.2. Specifying the types of objects to scan

By specifying the types of objects to scan, you establish which file formats, files sizes, and drives will be scanned for viruses when this task runs.

The file types scanned are defined in the **File types** section (see Figure 65). Select one of the three options:

- **Scan all files**. With this option, all objects will be scanned without exception.
- **Scan programs and documents (by content)**. If you select this group of programs, only potentially infected files will be scanned – files into which a virus could imbed itself.

  Note:

  There are files in which viruses cannot insert themselves, since the contents of such files does not contain anything for the virus to hook onto. An example would be .txt files.

  And vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of insertion and activation of malicious code in such files is fairly high.

  Before searching for viruses in an object, its internal header is analyzed for the file format (txt, doc, exe, etc.).

- **Scan programs and documents (by extension)**. In this case, the program will only scan potentially infected files, and in doing so, the file format will be determined by the filename's extension. Using the link, you can review a list of file extensions that are scanned with this option (see A.1 on pg. 302).

Tip:

Do not forget that someone could send a virus to your computer with the extension .txt that is actually an executable file renamed as a .txt file. If you select the **Scan programs and documents (by extension)** option, the scan would skip such a file. If the **Scan programs and documents (by contents)** is selected, the program will analyze file headers, discover that the file is an .exe file, and thoroughly scan it for viruses.

In the **Productivity** section, you can specify that only new files and those that have been modified since the previous scan or new files should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To do so, you must check **Scan only new and changed files**. This mode extends to simple and compound files.

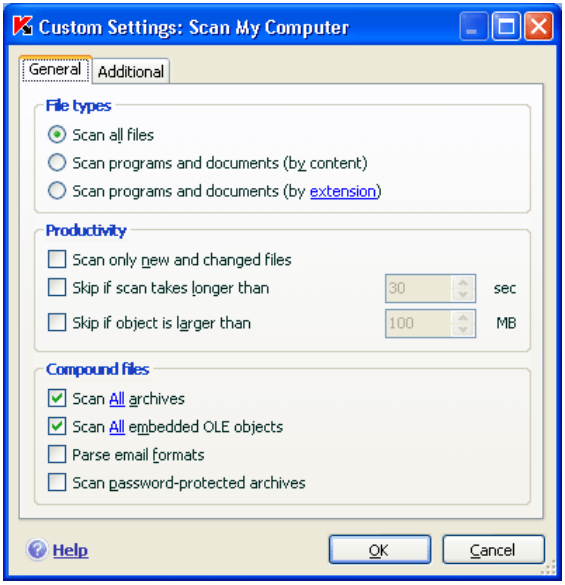


Figure 65. Configuring scan settings

You can also set time and file size limits for scanning in the **Productivity** section.

Skip if scan takes longer than... secs. Check this option and enter the maximum scan time for an object. If this time is exceeded, this object will be removed from the scan queue.

Skip if object is larger than…MB. Check this option and enter the maximum size for an object. If this size is exceeded, this object will be removed from the scan queue.

In the **Compound files** section, specify which compound files will be analyzed for viruses:

Scan All/Only New archives – scan .rar, .arj, .zip, .cab, .lha, .jar, and .ice archives.

Warning!

Kaspersky Anti-Virus does not delete compressed file formats that it does not support (for example, .ha, .uue, .tar) automatically, even if you select the option of automatically curing or deleting if the objects cannot be cured.

To delete such compressed files, click the Delete archives link in the dangerous object detection notification. This notification will be displayed on the screen after the program begins processing objects detected during the scan. You can also delete infected archives manually.

Scan all/only new embedded OLE objects– scan objects imbedded in files (for example, Excel spreadsheets or a macro imbedded in a Microsoft Word file, email attachments, etc.).

You can select and scan all files or only new ones for each type of compound file. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

Parse email formats – scan email files and email databases. If this checkbox is enabled, Kaspersky Anti-Virus dissects the mail format file and analyzes each component of the e-mail (body, attachments, etc.) for viruses. If this box is not checked, the file format file will be scanned as a single object.

Please note, when scanning password-protected email databases:

- Kaspersky Anti-Virus for Windows Workstations detects malicious code in Microsoft Office Outlook 2000 databases but does not disinfect them;
- Kaspersky Anti-Virus for Windows Workstations does not support scans for malicious code in Microsoft Office Outlook 2003 protected databases.

Scan password-protected archives – scans password protected archives. With this feature, a window will request a password before scanned archived objects. If this box is not checked, password-protected archives will be skipped.

14.4.3. Restoring default scan settings

When configuring scan task settings, you can always return to the recommended settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default scan settings:

1. Select the task name in the **Scan** section of the main window and use the Settings link to open the task settings window.

2. Click the **Default** button in the **Security Level** section.

14.4.4. Selecting actions for objects

If a file is found to be infected or suspicious during a scan, the program's next steps depend on the object status and the action selected.

One of the following statuses can be assigned to the object after the scan:

- Malicious program status (for example, *virus, Trojan*).
- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the code in the file contains a section of code that resembles a known but modified virus, or is reminiscent of the structure of a virus sequence.

By default, all infected files are disinfected, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select the task name in the **Scan** of the main program window and use the Settings link to open the task settings window. The possible responses are displayed in the appropriate sections(see Figure 66).

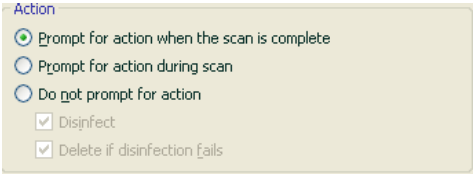

Action
Prompt for action when the scan is complete
Prompt for action during scan
Do not prompt for action
Disinfect
Delete if disinfection fails

Figure 66. Selecting actions for dangerous objects

If the action selected was	When it detects a malicious or potentially infected object
Prompt for action when the scan is complete	The program does not process the objects until the end of the scan. When the scan is complete, the statistics window will pop up with a list of objects detected, and you will be asked if you want to process the objects.
Prompt for action during the scan	The program will issue a warning message containing information about what malicious code has infected or

If the action selected was	When it detects a malicious or potentially infected object
	potentially infected the file, and gives you the choice of one of the following actions.
Do not prompt for action	The program records information about objects detected in the report without processing them or notifying the user. You are advised not to use this feature, since infected and potentially infected objects stay on your computer and it is practically impossible to avoid infection.
Do not prompt for action **Disinfect**	The program attempts to treat the object detected without asking the user for confirmation. If disinfection fails, the file will be assigned the status of *potentially infected*, and it will be moved to Quarantine (see 17.1 on pg. 218). Information about this is recorded in the report (see 17.3 on pg. 224). Later you can attempt to disinfect this object.
Do not prompt for action **Disinfect** **Delete if disinfection fails**	The program attempts to treat the object detected without asking the user for confirmation. If the object cannot be disinfected, it is deleted.
Do not prompt for action **Disinfect** **Delete**	The program automatically deletes the object

Before treating or deleting an object, Kaspersky Anti-Virus for Windows Workstations creates a backup copy of it, and sends it to Backup (see 17.2 on pg. 222) in case the object needs to be restored or an opportunity arises later to treat it.

14.4.5. Additional virus scan settings

In addition to configuring the basic virus scan settings, you can also use advanced settings (see Figure 67):

Enable iChecker technology – uses technology that can increase the scan speed by excluding certain objects from the scan. An object is excluded from the scan using a special algorithm that takes into account the release date of the threat signatures, the date the object was last scanned, and modifications to scan settings.

For example, you have an archived file that the program scanned and assigned the status of *not infected*. The next time, the program will skip this archive, unless it has been modified or the scan settings have been changed. If the structure of the archive has changed because a new object has been added to it, if the scan settings have changed, or if the threat signatures have been updated, the program will scan the archive again.
There are limitations to iChecker™: it does not work with large files and only applies to objects with a structure that Kaspersky Anti-Virus for Windows Workstations recognizes (for example, *.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar*).

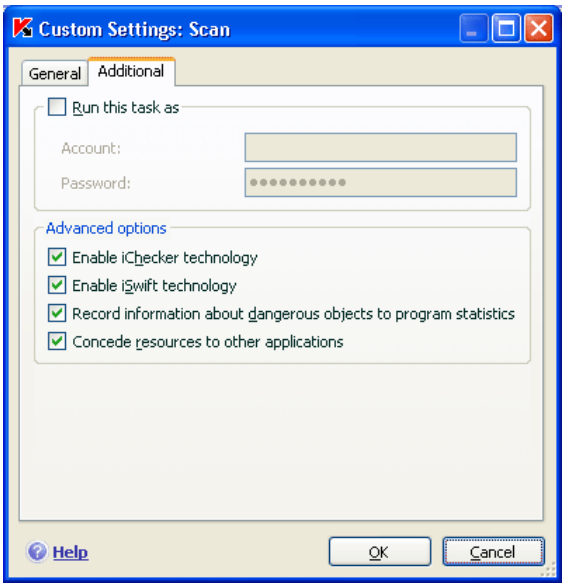


Figure 67. Advanced scan settings

Enable iSwift technology. This technology is a development of iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific location for the file in the file system and can only be applied to objects in an NTFS file system.

> iSwift technology is not available on computers running Microsoft Windows 98SE/ME/XP64.

Record information about dangerous objects to program statistics – save information about detected dangerous objects to general program statistics and display a list of threats detected during the scan on the **Detected** tab of the report (see 17.3.2 on pg. 227) window. If this option is disabled the information about dangerous objects will not be displayed in the report and it will be impossible to process data.

Concede resources to other applications – pause that virus scan task if the processor is busy with other applications.

14.4.6. Setting up global scan settings for all tasks

Each scan task is executed according to its own settings. By default, the tasks created when you install the program on your computer use the settings recommended by Kaspersky Lab.

You can configure global scan settings for all tasks. You will use a set of properties used to scan an individual object for viruses as a starting point.

To assign global scan settings for all tasks:

1. Select the **Scan** section in the left-hand part of the main program window and click Settings.
2. In the settings window that opens, configure the scan settings: Select the security level (see 14.4.1 on pg. 192), configure advanced level settings, and select an action (see 14.4.4 on pg. 196) for objects.
3. To apply these new settings to all tasks, click the **Apply** button in the **Other scan tasks** section. Confirm the global settings that you have selected in the popup dialogue box.

CHAPTER 15. TESTING KASPERSKY ANTI-VIRUS FEATURES

After installing and configuring Kaspersky Anti-Virus, we recommend that you verify that settings and program operation are correct using a test virus and variations of it.

15.1. The EICAR test virus and its variations

The test virus was specially developed by eicar (The European Institute for Computer Antivirus Research) for testing antivirus functionality.

The test virus IS NOT A VIRUS and does not contain program code that could damage your computer. However, most antivirus programs will identify it as a virus.

Never use real viruses to test the functionality of an antivirus!

You can download the test virus from the official **EICAR** website: http://www.eicar.org/anti_virus_test_file.htm.

The file that you downloaded from the **EICAR** website contains the body of a standard test virus. Kaspersky Anti-Virus will detected, label it a **virus**, and take the action set for that object type.

To test the reactions of Kaspersky Anti-Virus when different types of objects are detected, you can modify the contents of the standard test virus by adding one of the prefixes in the table shown here.

Prefix	Test virus status	Corresponding action when the application processes the object
No prefix, standard test virus	The file contains a test virus. You cannot disinfect the object.	The application will identify the object as malicious and not subject to treatment and will delete it.

Prefix	Test virus status	Corresponding action when the application processes the object
CORR–	Corrupted.	The application could access the object but could not scan it, since the object is corrupted (for example, the file structure is breached, or it is an invalid file format).
SUSP– WARN–	The file contains a test virus (modification). You cannot disinfect the object.	This object is a modification of a known virus or an unknown virus. At the time of detection, the threat signature databases do not contain a description of the procedure for treating this object. The application will place the object in Quarantine to be processed later with updated threat signatures.
ERRO–	Processing error.	An error occurred while processing the object: the application cannot access the object being scanned, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is being scanned on a network drive).
CURE–	The file contains a test virus. It can be cured. The object is subject to disinfection, and the text of the body of the virus will change to CURE.	The object contains a virus that can be cured. The application will scan the object for viruses, after which it will be fully cured.

Prefix	Test virus status	Corresponding action when the application processes the object
DELE-	The file contains a test virus. You cannot disinfect the object.	This object contains a virus that cannot be disinfected or is a Trojan. The application deletes these objects.

The first column of the table contains the prefixes that need to be added to the beginning of the string for a standard test virus. The second column describes the status and reaction of Kaspersky Anti-Virus to various types of test virus. The third column contains information on objects with the same status that the application has processed.

Values in the anti-virus scan settings determine the action taken on each of the objects.

15.2. Testing File Anti-Virus

To test the functionality File Anti-Virus;

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 15.1 on pg. 200), and the modifications of the test virus that you created.
2. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check **Log non-critical events** in the report settings window.
3. Run the test virus or a modification of it.

File Anti-Virus will intercept your attempt to access the file, will scan it, and will inform you that it has detected a dangerous object:

When you select different options for dealing with detected objects, you can test File Anti-Virus's reaction to detecting various object types.

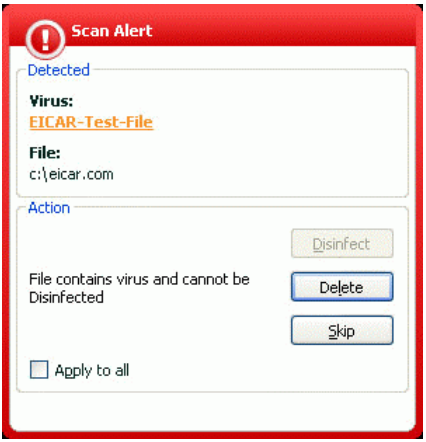
You can view details on File Anti-Virus performance in the report on the component.

15.3. Testing Virus scan tasks

To test Virus scan tasks:

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 15.1 on pg. 200), and the modifications of the test virus that you created.
2. Create a new virus scan task (see 14.3 on pg. 190) and select the folder containing the set of test viruses as the objects to scan (see 14.2 on pg. 188).
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check **Log non-critical events** in the report settings window.
4. Run the virus scan task (see 14.1 on pg. 188).

When you run a scan, as suspicious or infected objects are detected, notifications will be displayed on screen will information about the objects, prompting the user for the next action to take:



This way, by selecting different options for actions, you can test Kaspersky Anti-Virus reactions to detecting various object types.

You can view details on virus scan task performance in the report on the component.

CHAPTER 16. PROGRAM UPDATES

Keeping your anti-virus software up-to-date is an investment in your computer's security. Because new viruses, Trojans, and malicious software emerge daily, it is important to regularly update the application to keep your information constantly protected.

Updating the application involves the following components being downloaded and installed on your computer:

- **Threat signatures, network attack signatures, and network drivers**

  Information on your computer is protected using a database containing threat signatures and network attack profiles. The protection components that provide protection use the database of threat signatures to search for and disinfect harmful objects on your computer. The signatures are added to every hour, with records of new threats and methods to combat them. Therefore, it is recommended that they are updated on a regular basis.

  In addition to the threat signatures and the network attack database, network drivers that enable protection components to intercept network traffic are updated.

  Previous versions of Kaspersky Lab applications have supported *standard* and *extended* database sets. Each database dealt with protecting your computer against different types of dangerous objects. In Kaspersky Anti-Virus for Windows Workstations you don't need to worry about selecting the appropriate threat signature set. Now our products use an threat signatures that protect you from both malicious and potentially dangerous objects, and from hacker attacks.

- **Application modules**

  In addition to the signatures, you can upgrade the modules for Kaspersky Anti-Virus. New application updates appear regularly.

The main update source for Kaspersky Anti-Virus for Windows Workstations is Kaspersky Lab's update servers.

To download available updates from the update servers, your computer must be connected to the Internet.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00, +7 (495) 645-79-39 or, +7 (495) 956-70-00 to

request contact information for Kaspersky Lab partners, who can provide you with zipped updates on floppy disks or CDs.

Updates can be downloaded in one of the following modes:

- *Automatically*. Kaspersky Anti-Virus checks the update source for updates at specified intervals. During virus outbreaks, the check frequency may increase, and decrease when they are gone. If it finds new updates, Anti-Virus downloads them and installs them on the computer. This is the default setting.
- *By schedule*. Updating is scheduled to start at a specified time.
- *Manually*. With this option, you launch the Updater manually.

During updating, the application compares the threat signatures and application modules on your computer with the versions available on the update server. If your computer has the latest version of the signatures and application modules, you will see a notification window confirming that your computer is up-do-date. If the signatures and modules on your computer differ from those on the update server, only the missing part of the updates will be downloaded. The Updater does not download threat signatures and modules that you already have, which significantly increases download speed and saves Internet traffic.

Before updating threat signatures, Kaspersky Anti-Virus for Windows Workstations creates backup copies of them, that can be used if a rollback (see 16.2 on pg. 207) is required. If, for example, the update process corrupts the threat signatures and leaves them unusable, you can easily roll back to the previous version and try to update the signatures later.

You can distribute the updates retrieved to a local source while updating the application (see 16.4.4 on pg. 215). This feature allows you to update databases and modules used by 6.0 applications on networked computers to conserve bandwidth.

16.1. Starting the Updater

You can begin the update process at any time. It will run from the update source that you have selected (see 16.4.1 on pg. 209).

You can start the Updater from:

- the context menu (see 4.2 on pg. 49).
- from the program's main window (see 4.3 on pg. 50)

To start the Updater from the shortcut menu:

1. Right click the application icon in the system tray to open the shortcut menu.

2. Select **Update**.

To start the Updater from the main program window:

1. Select **Update** in the **Service** section.
2. Click the **Update now!** Button in the right panel of the main window or use the button on the status bar.

The update progress will be displayed in a special window, which can be hidden by clicking **Close**. The update will continue with the window hidden.

Note that updates are distributed to the local source during the update process, provided that this service is enabled (see 16.4.4 on pg. 215).

16.2. Rolling back to the previous update

Every time you start the Updater, Kaspersky Anti-Virus for Windows Workstations creates a backup copy of the current threat signatures before it starts downloading updates. This way you can return to using the previous version of signatures if an update fails.

To rollback to the previous version of threat signatures:

1. Select the **Update** component in the **Service** section of the main program window.
2. Click the **Rollback** button in the right panel of the main program window.

16.3. Creating update tasks

Kaspersky Anti-Virus has a built-in update task for updating program modules and threat signatures. You can also create your own update tasks with various settings and start schedules.

For example, you installed Kaspersky Anti-Virus on a laptop that you use at home and at your office. At home, you update the program from the Kaspersky Lab update servers, and at the office, from a local folder that stores the updates you need. Use two different tasks to avoid having to change update settings every time you change locations.

To create an advanced update task:

1. Select **Update** from the **Service** section of the main program window, open the context menu by right-clicking, and select **Save as**.
2. Enter the name for the task in the window that opens and click **OK**. A task with that name will then appear in the **Service** section of the main program window.

Warning!

Kaspersky Anti-Virus has a limit to the number of update tasks that the user can create. The maximum is two tasks.

The new task inherits all the properties of the task it is based on, except for the schedule settings. The default automatic scan setting for the new task is disabled.

After creating the task, configuring advanced settings: specify the update source (see 16.4.1 on pg. 208), network connection settings (see 16.4.3 on pg. 213), and if necessary, enable tasks under another profile (see 6.4 on pg. 81) and configure the schedule (see 6.5 on pg. 82).

To rename a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will then be changed in the **Service** section.

To delete a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Rename**.

Confirm that you want to delete the task in the confirmation window. The task will then be deleted from the list of tasks in the **Service** section.

Warning!

You can only rename and delete tasks that you have created.

16.4. Configuring update settings

The Updater settings specify the following parameters:

- The source from which the updates are downloaded and installed (see 16.4.1 on pg. 209)
- Application update mode and the specific items updated (see 16.4.2 on pg. 211);

- Update frequency if updates run on schedule (see 6.5 on pg. 82);
- Account under which the update will run (see 6.4 on pg. 81);
- The requirement to copy downloaded updates to a local directory (see 16.4.4 on pg. 215).
- What actions are to be performed after updating is complete (see 16.4.5 on pg. 216)

The following sections examine these aspects in detail.

16.4.1. Selecting an update source

The *update source* is some resource, containing updates for the threat signatures and Kaspersky Anti-Virus application modules.

You can use the following as update sources:

- *Administration Server* – a centralized update repository located on the Kaspersky Administration Kit Administration Server (for more details, see the Administrator User's Guide for Kaspersky Administration Kit).
- *Kaspersky Lab's update servers* – special web sites containing available updates for the threat signatures and application modules for all Kaspersky Lab products.
- *FTP or HTTP server or local or network folder* – local server or folder that contains the latest updates.

If you cannot access Kaspersky Lab's update servers (for example, you have no Internet connection), you can call the Kaspersky Lab main office at +7 (495) 797-87-00, +7 (495) 645-79-39 or +7 (495) 956-70-00 to request contact information for Kaspersky Lab partners, who can provide zipped updates on floppy disks or CDs.

Warning!

When requesting updates on removable media, please specify whether you want to have the updates for application modules as well.

You can copy the updates from a disk and upload them to a FTP or HTTP site, or save them in a local or network folder.

Select the update source on the **Update source** tab (see Figure 68).

By default, the updates are downloaded from Kaspersky Lab's update servers. The list of addresses which this item represents cannot be edited. When updating, Kaspersky Anti-Virus for Windows Workstations calls this list, selects the address of the first server, and tries to download files from this server. If

updates cannot be downloaded from the first server, the application tries to connect to each of the servers in turn until it is successful.

To download updates from another FTP or HTTP site:

1. Click **Add.**
2. In the **Select Update Source** dialog box, select the target FTP or HTTP site or specify the IP address, character name, or URL address of this site in the **Source** field. When selecting an ftp site as an update source, authentication settings must be entered in the URL of the server in the format ftp://user:password@server.

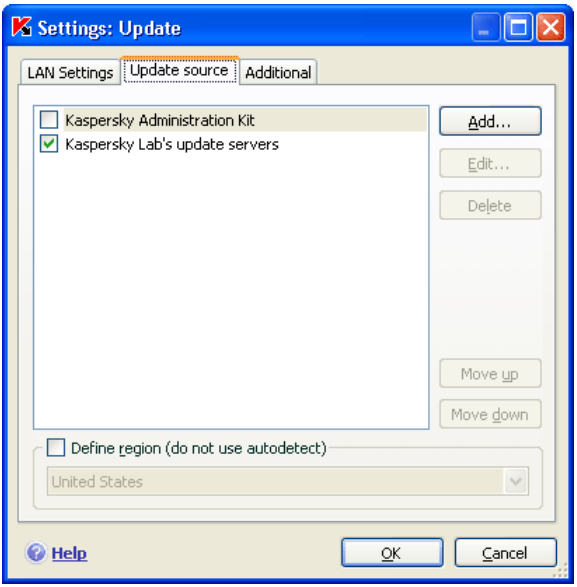


Figure 68. Selecting an update source

Warning!

If you selected a resource outside the LAN for updates, you will need an Internet connection to retrieve the updates.

To update from a local folder:

1. Click **Add.**
2. In the **Select Update Source** dialog box, select a folder or specify the full path to this folder in the **Source** field.

Kaspersky Anti-Virus for Windows Workstations adds new update sources at the top of the list, and automatically enables the source, by checking the box beside the source name.

If several resources are selected as update sources, the application tries to connect to them one after another, starting from the top of the list, and retrieves the updates from the first available source. You can change the order of sources in the list using the **Move up** and **Move down** buttons.

To edit the list, use the **Add**, **Edit** and **Remove** buttons. The only source you cannot edit or delete is the one labeled Kaspersky Lab's update servers.

If you use Kaspersky Lab's update servers as the update source, you can select the optimal server location for downloading updates. Kaspersky Lab has servers in several countries. Choosing the Kaspersky Lab update server closest to you will save you time and download updates faster.

To choose the closest server, check ☑ **Define region (do not use autodetect)** and select the country closest to your current location from the dropdown list. If you check this box, updates will run taking the region selected in the list into account. This checkbox is deselected by default and information about the current region from the operating system registry is used.

16.4.2. Selecting an update method and what to update

When configuring updating settings, it is important to define what will be updated and what update method will be used.

Update objects (see Figure 69) are the components that will be updated:

- threat signatures
- network drivers that enable protection components to intercept network traffic
- network attack databases used by Anti-Hacker
- program modules

The threat signatures, network drivers, and network attack database are always updated, whereas the application modules are updated only if the corresponding mode is selected.

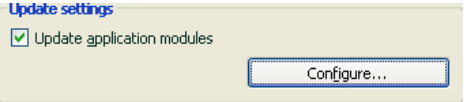


Figure 69. Selecting update objects

If you want to download and install updates for program modules:

Check **Update program modules** in the **Update Settings** dialog box of the **Update** service.

If there is an application module update on the update source, the application will download the required updates and apply them after the system is restarted. Downloaded module updates will not be installed until the computer is restarted.

If the next program update occurs before the computer is restarted and the previously downloaded application module updates are installed, threat signatures only will be updated.

Update method (see Figure 70) defines how the Updater is started. You can select one of these methods in the **Run mode** section:

Automatically. Kaspersky Anti-Virus checks the update source for updates at specified intervals. If it finds new updates, Anti-Virus downloads them and installs them on the computer. This mode is used by default.

If a network resource is specified as an update source, Kaspersky Anti-Virus for Windows Workstations tries to launch updating after a certain amount of time has elapsed as specified in the previous update package. If a local folder is selected as an update source, the application tries to download the updates from the local folder at a frequency specified in the update package that was downloaded during the last updating. This option allows Kaspersky Lab to regulate the updating frequency in case of virus outbreaks and other potentially dangerous situations. Your application will receive the latest updates for the threat signatures, network attacks, and software modules in a timely manner, thus excluding the possibility for malicious software to penetrate your computer.

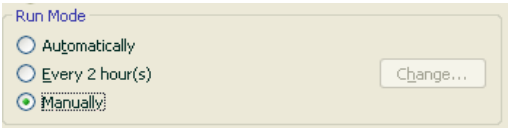


Figure 70. Selecting an update run mode

By schedule. Updating is scheduled to start at a specified time. By default, scheduled updates will occur every 2 hours. To edit the default schedule,

click the **Change...** button near the mode title and make the necessary changes in the window that opens (for more details, see 6.5 on pg. 82).

Manually. With this option, you start the Updater manually. Kaspersky Anti-Virus for Windows Workstations notifies you when it needs to be updated:

- A popup message, informing you that updating is required, appears above the application icon in the system tray (if notices are enabled; see 17.11.1 on pg. 254)
- The second indicator in the main program window informs you that your computer is out-of-date (see 5.1.1 on pg. 56)
- A recommendation, that the application needs updating, appears in the message section in the main program window (see 4.3 on pg. 50)

16.4.3. Configuring connection settings

If you set up the program to retrieve updates from Kaspersky Lab's update servers, or from other FTP or HTTP sites, you are advised to first check your connection settings.

All settings are grouped on a special tab – **LAN Settings**(see Figure 71).

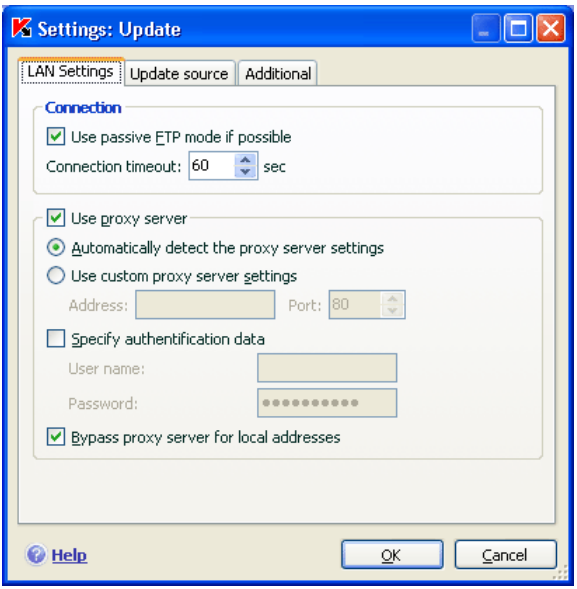


Figure 71. Configuring network update settings

Check **Use passive FTP mode if possible** if you download the updates from an FTP server in passive mode (for example, through a firewall). If you are working in active FTP mode, clear this checkbox.

In the **Connection timeout (sec)** field, assign the time allotted for connection with the update server. If the connection fails, once this time has elapsed the program will attempt to connect to the next update server. This continues until a connection is successfully made or until all the available update servers are attempted.

Check **Use proxy server** if you are using a proxy server to access the Internet and, if necessary, select the following settings:

- Select the proxy server settings that will be used during updating:

  Automatically detect the proxy server settings. If you select this option, the proxy settings are detected automatically using WPAD (Web Proxy Auto-Discovery Protocol). If this protocol cannot detect the address, Kaspersky Anti-Virus will use the proxy server settings specified in Microsoft Internet Explorer.

  Use custom proxy settings – Use a proxy that is different from that specified in the browser connection settings. In the **Address** field, enter either the IP address or the symbolic name of the proxy server, and specify the number of the proxy port in the **Port** field.

- Specify whether authentication is required on the proxy server. *Authentication* is the process of verifying user registration data for access control purposes.

  If authentication is required to connect to the proxy server, check **Specify authentification data** and specify the username and password in the fields below. In this event, first NTLM authentication and then BASIC authentication will be attempted.

  If this checkbox is not selected or if the data is not entered, NTLM authentication will be attempted using the user account used to start the update (see 6.4 on pg. 81).

  If the proxy server requires authentication and you did not enter the username and password or the data specified were not accepted by the proxy server for some reason, a window will pop up when updates start, asking for a username and password for authentication. If authentication is successful, the username and password will be used at next updates. Otherwise, the authentication settings will be requested again.

To avoid using a proxy when the update source is a local folder, select the **Bypass proxy server for local addresses**.

This feature is unavailable under Windows 9X/NT 4.0. However, the proxy server is by default not used for local addresses.

16.4.4. Update distribution

The update copying feature makes it possible to optimize the load on your business's network. Updates are copied in two stages:

1. One of the computers on the network retrieves an application and threat signature update package from the Kaspersky Lab web servers or from another web resource hosting a current set of updates. The updates retrieved are placed in a public access folder.
2. Other computers on the network access the public access folder to retrieve application updates.

To enable update distribution, select the **Update distribution folder** checkbox on the **Additional** tab (see Figure 72), and in the field below, specify the shared folder where updates retrieved will be placed. You can enter the path manually or selected in the window that opens when you click **Browse**. If the checkbox is selected, updates will automatically be copied to this folder when they are retrieved.

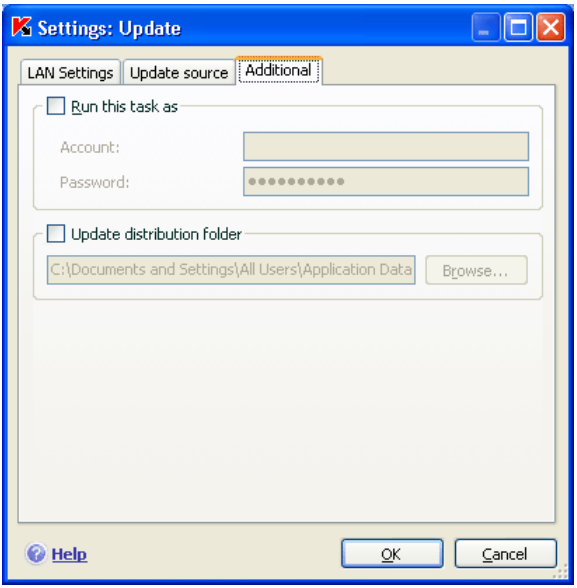


Figure 72. Copy updates tool settings

Note that Kaspersky Anti-Virus 6.0 only retrieves update packages for v. 6.0 applications from the Kaspersky Lab update servers. We recommend copying updates for other Kaspersky Lab applications through Kaspersky Administration Kit.

If you want other computers on the network to update from the folder that contains updates copied from the Internet, you must take the following steps:

1. Grant public access to this folder.
2. Specify the shared folder as the update source on the network computers in the Updater settings.

16.4.5. Actions after updating the program

Every threat signature update contains new records that protect your computer from the latest threats.

Kaspersky Lab recommends that you scan *quarantined objects* and *startup objects* each time after the database is updated.

Why these objects should be scanned?

The quarantine area contains objects that have been flagged by the program as suspicious or possibly infected (see 17.1 on pg. 218). Using the latest version of the threat signatures, Kaspersky Anti-Virus for Windows Workstations may be able to identify the threat and eliminate it.

By default, the application scans quarantined objects after each threat signature update. You are also advised to periodically view the quarantined objects because their statuses can change after several scans. Some objects can then be restored to their previous locations, and you will be able to continue working with them.

To disable scans of quarantined objects, uncheck **Rescan Quarantine** in the **Action after update** section.

Startup objects are critical for the safety of your computer. If one of them is infected with a malicious application, this could cause an operating system startup failure. Kaspersky Anti-Virus for Windows Workstations has a built-in scan task for startup objects (see Chapter 14 on pg. 187). You are advised to set up a schedule for this task so that it is launched automatically after each threat signature update (see 6.5 on pg. 82).

CHAPTER 17. ADVANCED OPTIONS

Kaspersky Anti-Virus for Windows Workstations has other features that expand its functionality.

The program places some objects in special storage areas, in order to ensure maximum protection of data with minimum losses.

- Backup contains copies of objects that Kaspersky Anti-Virus for Windows Workstations has changed or deleted (see 17.2 on pg. 222). If any object contained information that was important to you and could not be fully recovered during anti-virus processing, you can always restore the object from its backup copy.
- Quarantine contains potentially infected objects that could not be processed using the current threat signatures (see 17.1 on pg. 218).

It is recommended that you periodically examine the list of stored objects. Some of them may already be outdated, and some may have been restored.

The advanced options include a number of diverse useful features. For example:

- Technical Support provides comprehensive assistance with Kaspersky Anti-Virus for Windows Workstations (see 17.6 on pg. 244). Kaspersky provides you with several channels for support, including on-line support and a questions and comments forum for program users.
- The Notifications feature sets up user notifications about key events for Kaspersky Anti-Virus for Windows Workstations (see 17.11.1 on pg. 254). These could be either events of an informative nature, or critical errors that must be eliminated immediately.
- Self-Defense protects the program's own files from being modified or damaged by hackers, blocks remote administration from using the program's features, and restricts other users on your computer from performing certain actions in Kaspersky Anti-Virus for Windows Workstations (see 17.11.1.2 on pg. 257). For example, changing the level of protection can significantly influence information security on your computer.
- License Key Manager can obtain detailed information on the license used, activate your copy of the program, and manage license key files (see 17.5 on pg. 242).

The program also provides a Help section (see 17.4 on pg. 241) and detailed reports (see 17.3 on pg. 224) on the operation of all protection components and update and virus scan tasks.

Creating the monitored ports list can regulate which Kaspersky Anti-Virus for Windows Workstations modules control data transferred on select ports (see 17.7 on pg. 245).

The Rescue Disk allows restoring your computer's functionality after an infection (see 17.10 on pg. 250). This is particularly helpful when you cannot boot your computer's operating system after malicious code has damaged system files.

You can also change the appearance of Kaspersky Anti-Virus for Windows Workstations and can customize the program interface (see 17.9 on pg. 249).

The following sections discuss these features in more detail.

17.1. Quarantine for potentially infected objects

Quarantine is a special storage area that holds potentially infected objects.

Potentially infected objects are objects that are suspected of being infected with viruses or modifications of them.

Why *potentially infected*? This are several reasons why it is not always possible to determine whether an object is infected:

- The code of the object scanned resembles a known threat but is partially modified.

  Threat signatures contain threats that have already been studied by Kaspersky Lab. If a malicious program is modified by a hacker but these changes have not yet been entered into the signatures, Kaspersky Anti-Virus for Windows Workstations classifies the object infected with this changed malicious program as being potentially infected, and indicates what threat this infection resembles.

- The code of the object detected is reminiscent in structure of a malicious program, although nothing similar is recorded in the threat signatures.

  It is quite possible that this is a new type of threat, so Kaspersky Anti-Virus for Windows Workstations classifies the object as a potentially infected object.

The *heuristic code* analyzer detects potential viruses. This mechanism is fairly effective and very rarely produces false positives.

A potentially infected object can be detected and placed in quarantine by File Anti-Virus, Mail Anti-Virus, Proactive Defense or in the course of a virus scan.

You can place an object in quarantine by clicking **Quarantine** in the notification that pops up when a potentially infected object is detected.

When you place an object in Quarantine, it is moved, not copied. The object is deleted from the disk or email and is saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

17.1.1. Actions with quarantined objects

The total number of objects in Quarantine is displayed by selecting the **Data files** item in the **Service** area of the application's main window. In the right-hand part of the screen the *Quarantine* section displays:

- the number of potentially infected objects detected during Kaspersky Anti-Virus for Windows Workstations operation;
- the current size of Quarantine.

Here you can delete all objects in the quarantine with the **Clean up** button. Note that in doing so the Backup files and report files will also be deleted.

To access objects in Quarantine:

left-click in any part of the **Quarantine** section.

You can take the following actions on the **Quarantine** tab (see Figure 73):

- Move a file to Quarantine that you suspect is infected but the program did not detect. To do so, click **Add** and select the file in the standard selection window. It will be added to the list with the status *added by user*.

  If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status after the scan will not immediately be changed to *OK*. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

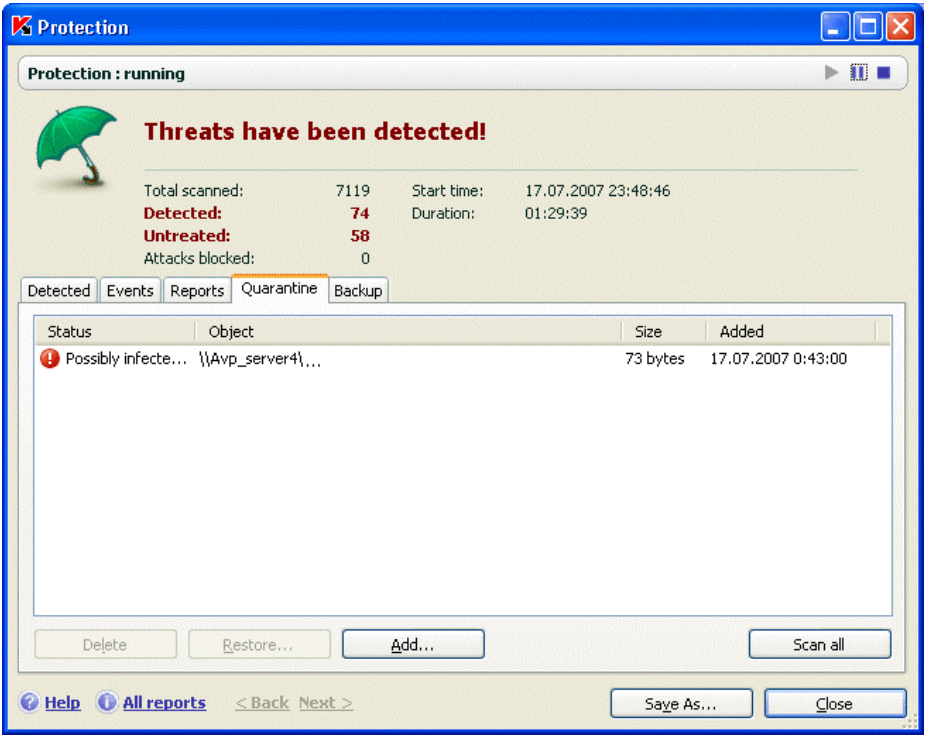


Figure 73. List of quarantined objects

- Scan and disinfect all potentially infected objects in Quarantine using the current threat signatures by clicking, click **Scan all**.

  After scanning and disinfecting any quarantined object, its status may change to *infected, potentially infected, false positive, OK,* etc.

  The *infected* status means that the object has been identified as infected but it could not be treated. You are advised to delete such objects.

  All objects marked *false positive* can be restored, since their former status as *potentially infected* was not confirmed by the program once scanned again.

- Restore the files to a folder selected by the user or their original folder prior to Quarantine (default). To restore an object, select it from the list and click **Restore**. When restoring objects from archives, email databases, and email format files placed in Quarantine, you must also select the directory to restore them to.

> Tip:
>
> We recommend that you only restore objects with the status *false positive, OK,* and *disinfected*, since restoring other objects could lead to infecting your computer.

- Delete any quarantined object or group of selected objects. Only delete objects that cannot be disinfected. To delete the objects, select them in the list and click **Delete**.

17.1.2. Setting up Quarantine

You can configure the settings for the layout and operation of Quarantine, specifically:

- Set up automatic scans for objects in Quarantine after each threat signature update (for more details, see 16.4.4 on pg. 215).

> Warning!
>
> The program will not be able to scan quarantined objects immediately after updating the threat signatures if you are accessing the Quarantine area.

- Set the maximum Quarantine storage time.

  The default storage time 30 days, at the end of which objects are deleted. You can change the Quarantine storage time or disable this restriction altogether.

To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. In the **Quarantine & Backup** section (see Figure 74), enter the length of time after which objects in Quarantine will be automatically deleted. Alternately, uncheck the checkbox to disable automatic deletion.

Figure 74. Configuring the Quarantine storage period

17.2. Backup copies of dangerous objects

Sometimes when objects are disinfected their integrity is lost. If a disinfected file contains important information which is partially or fully corrupted, you can attempt to restore the original object from a backup copy.

A **backup copy** is a copy of the original dangerous object that is created before the object is disinfected or deleted. It is saved in Backup.

Backup is a special storage area that contains backup copies of dangerous objects. Files in backup are saved in a special format and are not dangerous.

17.2.1. Actions with backup copies

The total number of backup copies of objects in Backup is displayed in the **Data files** in the **Service** section of the application's main window. In the right-hand part of the screen the *Backup* section displays:

- the number of backup copies of objects created by Kaspersky Anti-Virus for Windows Workstations
- the current size of Backup.

Here you can delete all the copies in Backup with the **Clean up** button. Note that in doing so the Quarantine objects and report files will also be deleted.

To access dangerous object copies:

left-click in any part of the **Backup** section.

A list of backup copies is displayed in the Backup tab (see **Error! Reference source not found.**). The following information is displayed for each copy: the path and filename of the object, the status of the object assigned by the scan, and its size.

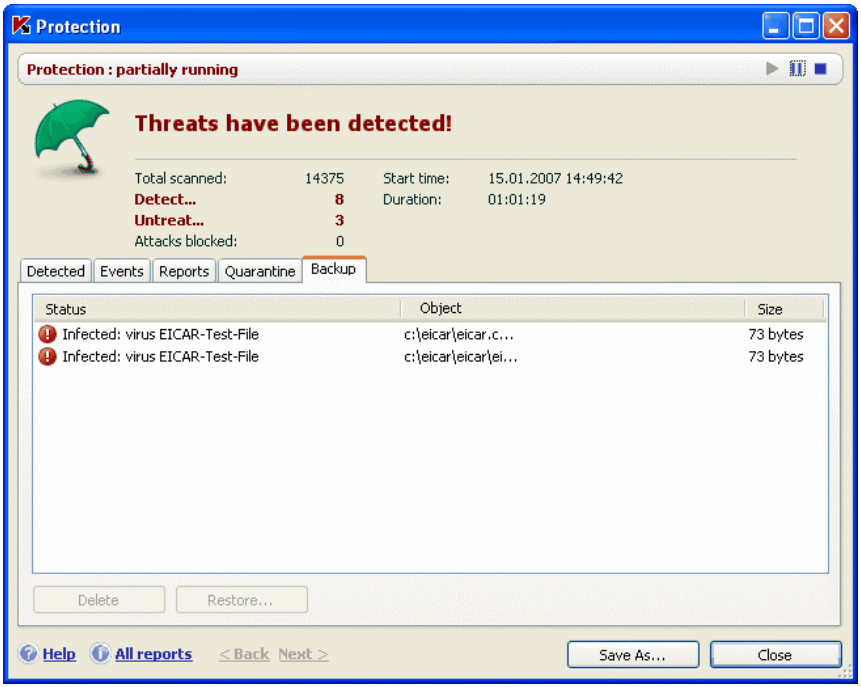


Figure 75. List of backuped objects

You can restore selected copies using the **Restore** button. The object is restored from Backup with the same name that it had prior to disinfection.

If there is an object in the original location with that name (this is possible if a copy was made of the object being restored prior to disinfection), a warning will be given. You can change the location of the restored object or rename it.

You are advised to scan backup objects for viruses immediately after restoring them. It is possible that with updated signatures you will be able to disinfect it without losing file integrity.

You are advised **not** to restore backup copies of objects unless absolutely necessary. This could lead to an infection on your computer.

You are advised to periodically examine the Backup area, and empty it using the **Delete** button. You can also set up the program so that it automatically deletes the oldest copies from Backup (see 17.2.2 on pg. 224).

17.2.2. Configuring Backup settings

You can define the maximum time that backup copes remain in the Backup area.

The default Backup storage time is 30 days, at the end of which backup copies are deleted. You can change the storage time or remove this restriction altogether. To do so:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. Set the duration for storing backup copies in the repository in the **Quarantine and Backup** section (see Figure 74) on the right-hand part of the screen. Alternately, uncheck the checkbox to disable automatic deletion.

17.3. Reports

Kaspersky Anti-Virus for Windows Workstations component actions, virus task scans and updates are all recorded in reports.

The total number of reports created by the program and their total size is displayed by clicking on **Data files** in the **Service** section of the main program window. The information is displayed in the *Reports* box.

To view reports:

Left-click anywhere in the *Reports* box to open the Protection window, which summarizes protection given by the application. The window will open to the **Reports** tab (see Figure 76).

The Reports tab lists the latest reports on all components and update and virus scan tasks run during the current session of Kaspersky Anti-Virus for Windows Workstations. The status is listed beside each component or task, for example, *stopped* or *complete*. If you want to view the full history of report creation for the current session of the program, check **Show report history**.

To review all the events reported for a component or task:

Select the name of the component or task on the **Reports** tab and click the **Details** button.

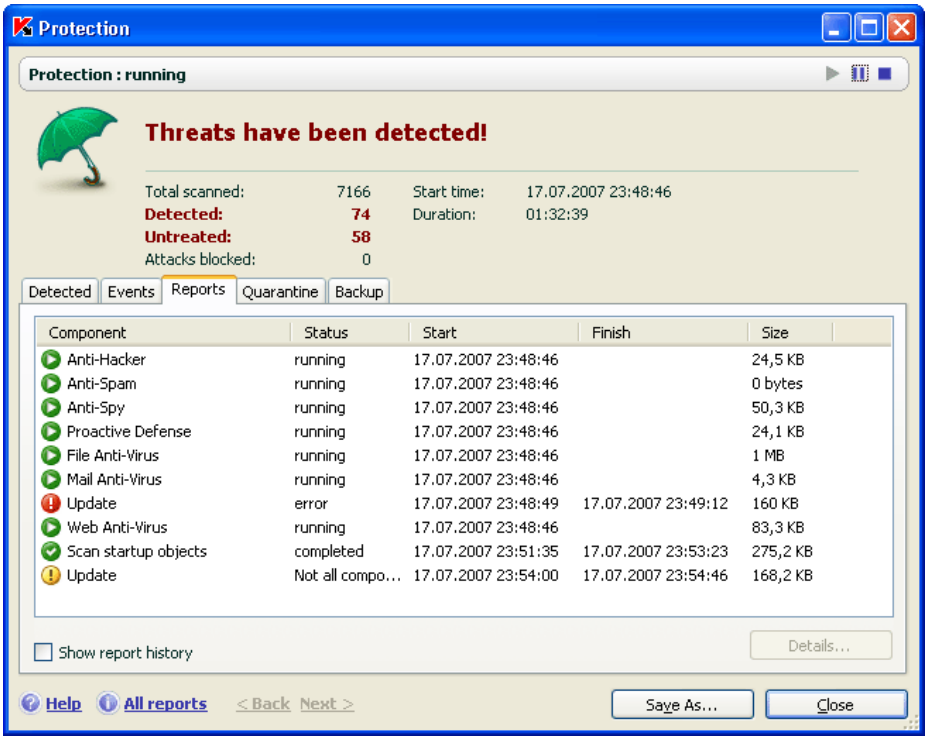


Figure 76. Reports on component operation

A window will then open that contains detailed information on the performance of the selected component or task. The resulting performance statistics are displayed in the upper part of the window, and detailed information is provided on the tabs. Depending on the component or task, the tabs can vary:

- The **Detected** tab contains a list of dangerous objects detected by a component or a virus scan task.
- The **Events** tab displays component or task events.
- The **Statistics** tab contains detailed statistics for all scanned objects.
- The **Settings** tab displays settings used by protection components, virus scans, or threat signature updates.
- The **Macros** and **Registry** tabs are only in the Proactive Defense report and contain information about all macros which attempted to run on your computer, and on all attempts to modify the operating system registry.

- The **Phishing Sites**, **Popup Windows**, **Banner Ads**, and **Dial Attempts** tabs are only in the Anti-Spy report. They contain information on all the phishing attacks detected and all the popup windows, banner ads, and autodial attempts blocked during that session of the program.
- The **Network Attacks**, **Banned Hosts**, **Application Activity**, and **Packet Filtering** tabs are only be found in the Anti-Hacker report. They include information on all attempted network attacks on your computer, hosts banned after attacks, descriptions of application network activity that matches existing activity rules, and all data packets that match Anti-Hacker packet filtering rules.
- The **Established Connections**, **Open Ports**, and **Traffic** tabs also cover network activity on your computer, displaying currently established connections, open ports, and the amount of network traffic your computer has sent and received.

You can export the entire report as a text file. This feature is useful when an error has occurred which you cannot eliminate on your own, and you need assistance from Technical Support. If this happens, the report must be sent as a .txt file to Technical Support to enable our specialists can study the problem in detail and solve it as soon as possible.

To export a report as a text file:

Click **Save as** and specify where you want to save the report file.

After you are done working with the report, click **Close**.

There is an **Actions** button on all the tabs (except **Settings** and **Statistics**) which you can use to define responses to objects on the list. When you click it, a context-sensitive menu opens with a selection of these menu items (the menu differs depending on the component – all the possible options are listed below):

Disinfect – attempts to disinfect a dangerous object. If the object is not successfully disinfected, you can leave it on this list to scan later with an updated threat signatures or delete it. You can apply this action either to one object on the list or to several selected objects.

Discard – delete the record of detecting the object from the list.

Add to trusted zone – exclude the object from protection. A window will open with an exclusion rule for the object.

Go to File – open the folder where the object is located in Windows Explorer.

Neutralize All – neutralize all objects on the list. Kaspersky Anti-Virus for Windows Workstations will attempt to process the objects using threat signatures.

Discard All – clear the report on detected objects. When you use this function, all detected dangerous objects remain on your computer.

Search www.viruslist.com – go to a description of the object in the Virus Encyclopedia on the Kaspersky Lab website.

Search www.google.com – find information on the object using this search engine.

Search – enter search terms for objects on the list by name or status.

In addition, you can sort the information displayed in the window in ascending and descending order for each of the columns, by clicking on the column head.

17.3.1. Configuring report settings

To configure settings for creating and saving reports:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. Edit the settings in the **Reports** box (see Figure 77) as follows:
   - Allow or disable logging informative events. These events are generally not important for security. To log events, check **Log non-critical events**;
   - Choose only to report events that have occurred since the last time the task was run. This saves disk space by reducing the report size. If **Keep only recent events** is checked, the report will begin from scratch every time you restart the task. However, only non-critical information will be overwritten.
   - Set the storage time for reports. By default, the report storage time is 30 days, at the end of which the reports are deleted. You can change the maximum storage time or remove this restriction altogether.

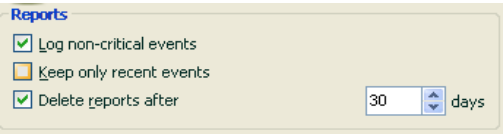


Figure 77. Configuring report settings

17.3.2. The *Detected* tab

This tab (see Figure 78) contains a list of dangerous objects detected by Kaspersky Anti-Virus for Windows Workstations. The full filename and path is

shown for each object, with the status assigned to it by the program when it was scanned or processed.

If you want the list to contain both dangerous objects and successfully neutralized objects, check **Show neutralized objects**.

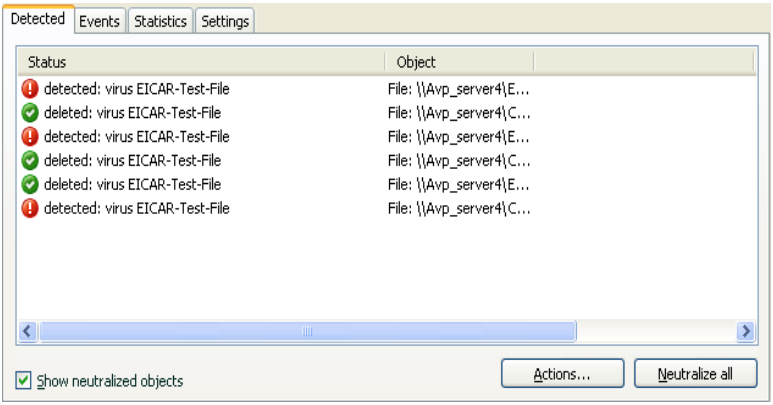


Figure 78. List of detected dangerous objects

To process dangerous objects detected by Kaspersky Anti-Virus, press the **Neutralize** button (for one object or a group of selected objects) or **Neutralize all** (to process all the objects on the list). After each object is processed, a message will appear on screen. Here you will have to decide what to do with them next.

If you check **Apply to all** in the notification window, the action selected will be applied to all objects with the status selected from the list before beginning processing.

17.3.3. The *Events* tab

This tab (see Figure 79) provides you with a complete list of all the important events in protection component operation, virus scans, and threat signature updates that were not overridden by an activity control rule (see 10.1.1 on pg. 121).

These events can be:

Critical events are events of a critical importance that point to problems in program operation or vulnerabilities on your computer. For example, *virus detected*, *error in operation*.

Important events are events that must be investigated, since they reflect important situations in the operation of the program. For example, *stopped.*

Informative messages are reference-type messages which generally do not contain important information. For example, *OK, not processed*. These events are only reflected in the event log if **Show all events** is checked.

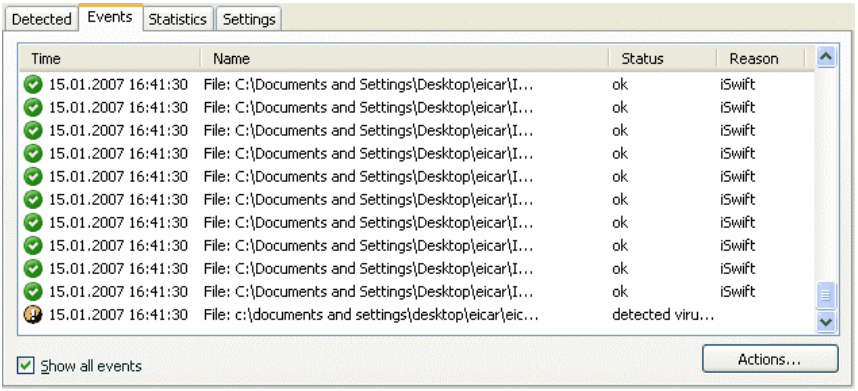


Figure 79. Events that take place in component operation

The format for displaying events in the event log may vary with the component or task. The following information is given for update tasks:

- Event name
- Name of the object involved in the event
- Time when the event occurred
- Size of the file loaded

For virus scan tasks, the event log contains the name of the object scanned and the status assigned to it by the scan/processing.

You can also train Anti-Spam while viewing the report using the special context menu. To do so, select the name of the email and open the context menu by right-clicking and select **Mark as Spam**, if the email is spam, or **Mark as Not Spam**, if the selected email is accepted email. In addition, based on the information obtained by analyzing the email, you can add to the Anti-Spam white and black lists. To do so, use the corresponding items on the context menu.

17.3.4. The *Statistics* tab

This tab (see Figure 80) provides you with detailed statistics on components and virus scan tasks. Here you can learn:

- How many objects were scanned for dangerous traits in this session of a component, or after a task is completed. The number of scanned archives, compressed files, and password protected and corrupted objects is displayed.
- How many dangerous objects were detected, not disinfected, deleted, or placed in Quarantine.

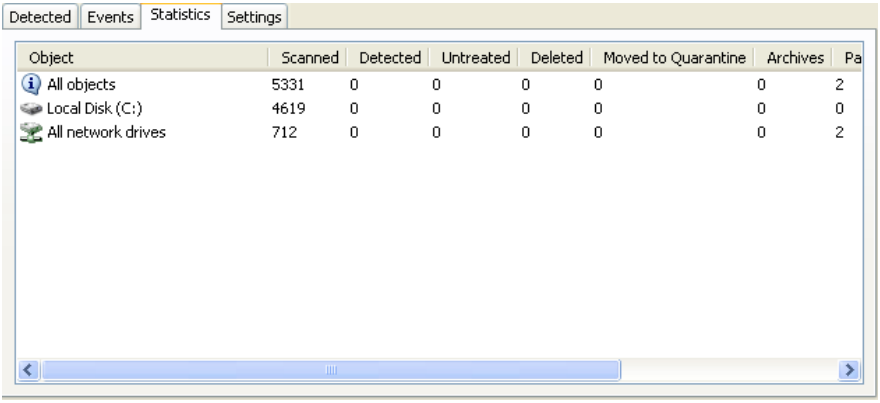


Figure 80. Component statistics

17.3.5. The *Settings* tab

The **Settings** tab (see Figure 81) displays a complete overview of the settings for protection components, virus scans and program updates. You can find out the current security level for a component or virus scan, what actions are being taken with dangerous objects, or what settings are being used for program updates. Use the Change settings link to configure the component.

You can configure advanced settings for virus scans:

- Establish the priority of scan tasks used if the processor is heavily loaded. The **Concede resources to other applications** checkbox is checked by default. With this feature, the program tracks the load on the processor and disk subsystems for the activity of other applications. If the load on the processor increases significantly and prevents the user's applications from operating normally, the program reduces scanning activity. This increases scan time and frees up resources for the user's applications.

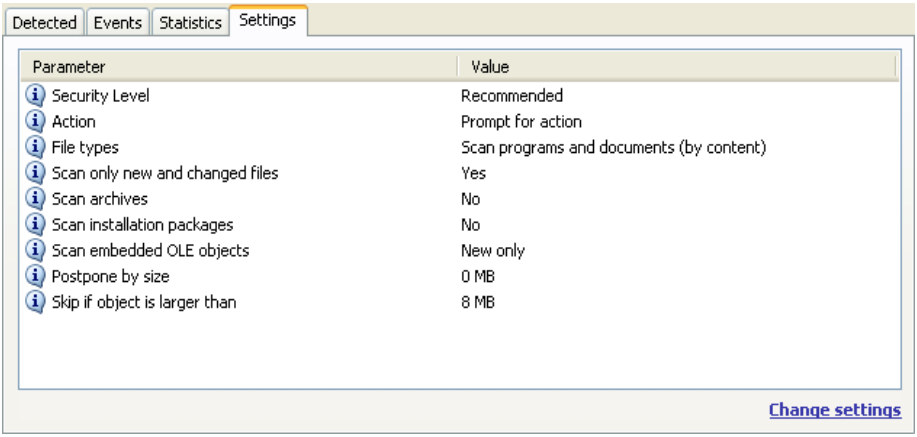


Figure 81. Component settings

- Set the computer's mode of operation for after a virus scan is complete. You can configure the computer to shut down, restart, or go into standby or sleep mode. To select an option, left-click on the hyperlink until it displays the option you need.

  You may need this feature if, for example, you start a virus scan at the end of the work day and do not want to wait for it to finish.

  However, to use this feature, you must take the following additional steps: before launching the scan, you must disable password requests for objects being scanned, if enabled, and enable automatic processing of dangerous objects, to disable the program's interactive features.

17.3.6. The *Macros* tab

All the macros that attempted to run during the current Kaspersky Anti-Virus for Windows Workstations session are listed on the **Macros** tab (see Figure 82). Here you will find the full name of each macro, the time it was executed, and its status after macro processing.

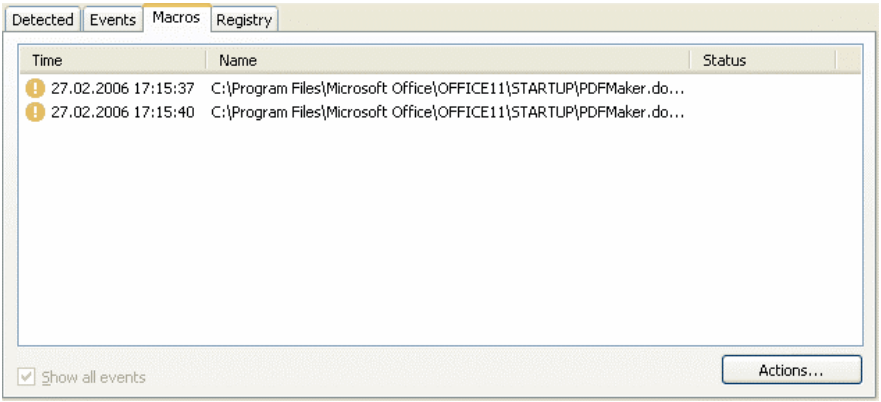


Figure 82. Detected dangerous macros

You can choose view mode for this tab. If you don't want to view informational events uncheck **Show all events**.

17.3.7. The *Registry* tab

The program records operations with registry keys that have been attempted since the program was started on the **Registry** tab (see Figure 83), unless forbidden by a rule (see 10.1.3.2 on pg. 129).

The tab lists the full name of the key, its value, the data type, and information about the operation that has taken place: what action was attempted, at what time, and whether it was allowed.

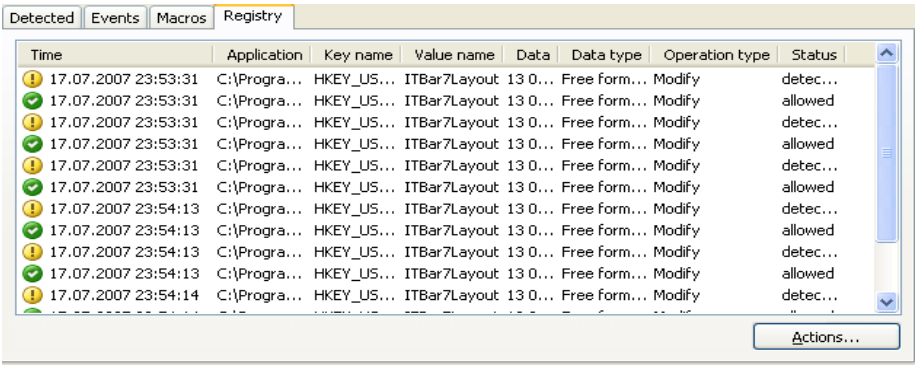


Figure 83. Read and modify system registry events

17.3.8. The *Phishing Sites* tab

This report tab (see Figure 84) displays all phishing attempts carried out during the current Kaspersky Anti-Virus for Windows Workstations session. The report lists a link to the phishing site detected in the email (or other source), the date and time that the attack was detected, and the attack status (whether it was blocked).

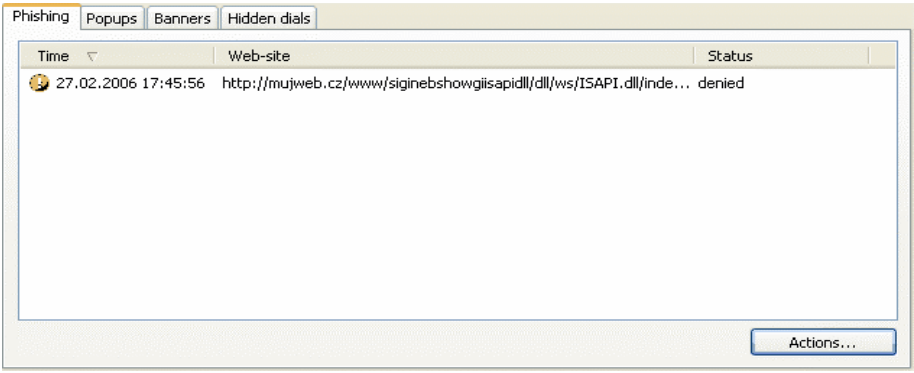


Figure 84. Blocked phishing attacks

17.3.9. The *Popup Windows* tab

This report tab (see Figure 85) lists the addresses of all the popup windows that Anti-Spy has blocked. These windows generally open from websites.

The address and date and time when Popup Blocker blocked the window are recorded for each popup.

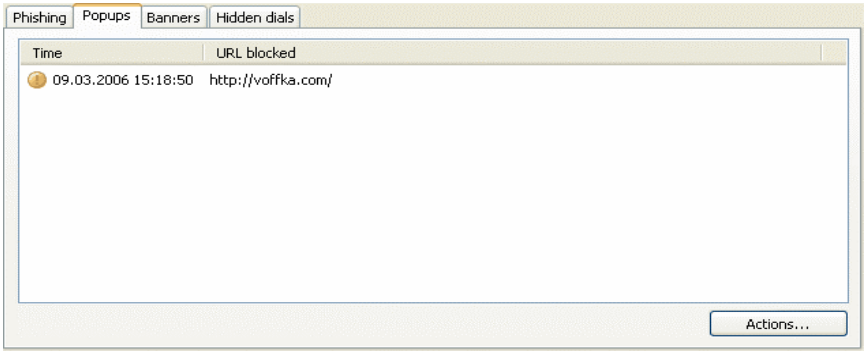


Figure 85. List of blocked popup windows

17.3.10. The *Banner Ads* tab

This report tab (see Figure 86) contains the addresses of the banner ads that Kaspersky Anti-Virus for Windows Workstations has detected in the current session. The web address for each banner ad is listed, along with the processing status (banner blocked or banner displayed).

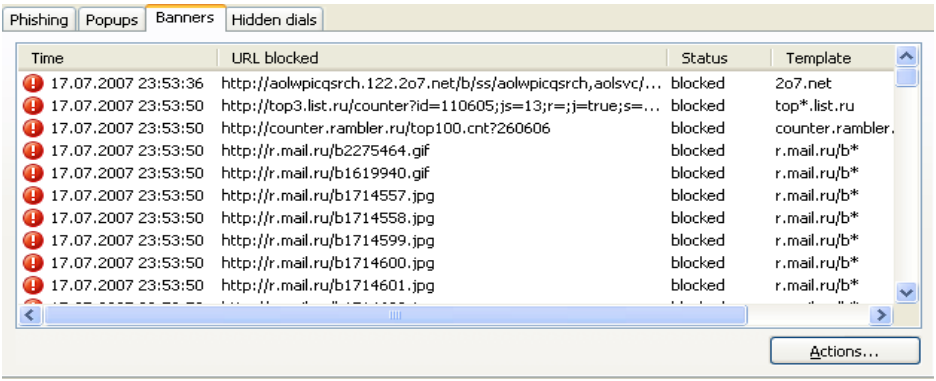


Figure 86. Blocked banner ad list

You can allow blocked banners to be displayed. To do so, select the object you want from the list and click **Actions** → **Allow**.

17.3.11. The *Dial Attempts* tab

This tab (see Figure 87) displays all secret dialer attempts to connect to paid websites. Such attempts are generally carried out by malicious programs installed on your computer.

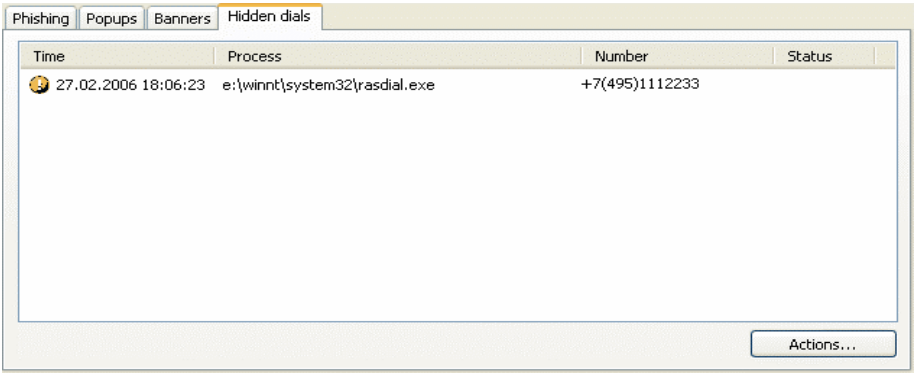


Figure 87. Dial attempt list

In the report, you can view what program attempted to dial the number to connect to the Internet, and whether the attempt was blocked or allowed.

17.3.12. The *Network Attacks* tab

This tab (see Figure 88) displays a brief overview of network attacks on your computer. This information is recorded if the Intrusion Detection System is enabled, which monitors all attempts to attack your computer.

The **Network attacks** tab lists the following information on attacks:

- Source of the attack. This could be an IP address, host, etc.
- Local port on which the attack on the computer was attempted.
- Brief description of the attack.
- The time when the attack was attempted.

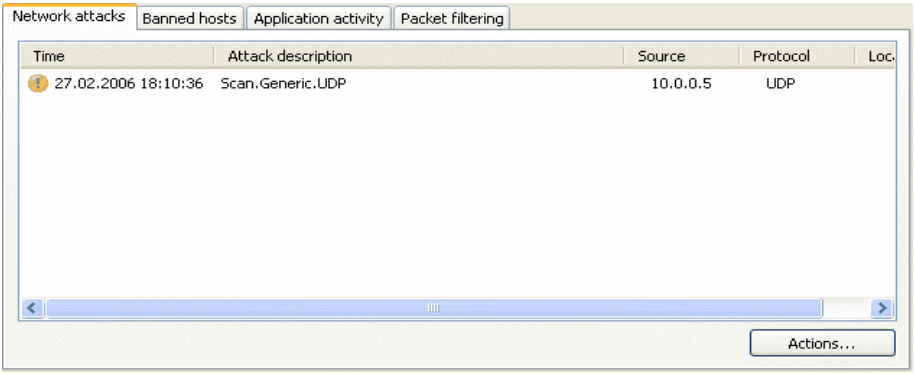


Figure 88. List of blocked network attacks

17.3.13. The *Banned Hosts* tab

All hosts which have been blocked after an attack was detected by the Intrusion Detection System are listed on this report tab (see Figure 89).

The name of each host and the time that it was blocked are shown. You can unblock a host on this tab. To do so, select the host on the list and click the **Actions → Unblock** button.

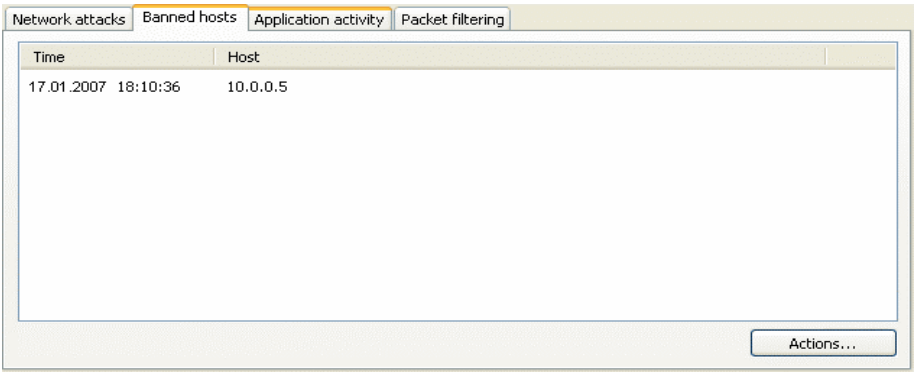


Figure 89. Blocked host list

17.3.14. The *Application Activity* tab

All applications whose activity matches application rules and has been recorded by the *Firewall* module during the current Anti-Hacker session, are listed on the **Application Activity** tab (see Figure 90).

Activity is only recorded if **Log event** flag is checked in the rule. In application rules included with Kaspersky Anti-Virus for Windows Workstations this flag is unchecked by default.

This tab displays the basic properties of each application (name, PID, rule name) and a brief summary of its activity (protocol, packet direction, etc.). Information is also listed about whether the application's activity is blocked.

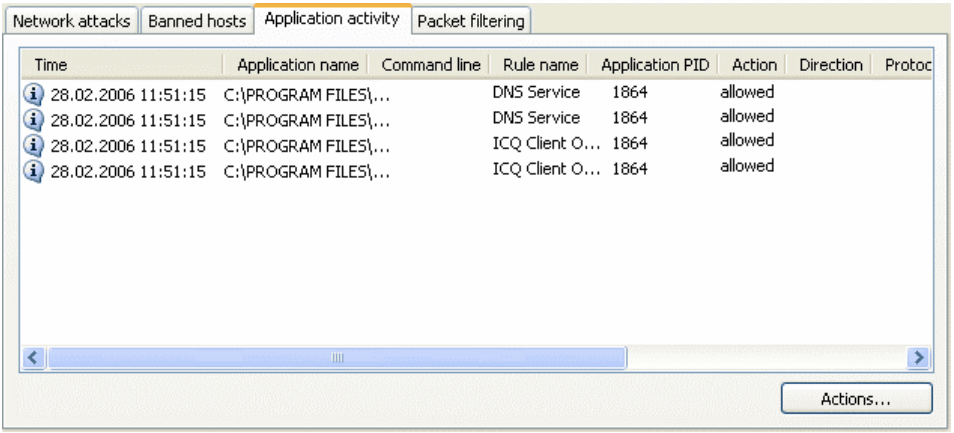


Figure 90. Monitored application activity

17.3.15. The Packet Filtering tab

The **Packet filtering** tab contains information about sending and receiving packets that match filtration rules and were logged during the current session of the application (see Figure 91).

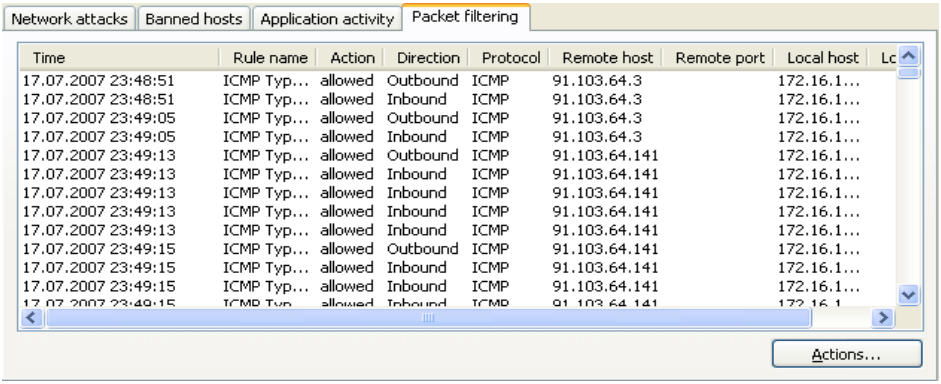

Network attacks
Banned hosts
Application activity
Packet filtering
Time
Rule name
Action
Direction
Protocol
Remote host
Remote port
Local host
17.07.2007 23:48:51 ICMP Typ... allowed Outbound ICMP 91.103.64.3 172.16.1...
17.07.2007 23:48:51 ICMP Typ... allowed Inbound ICMP 91.103.64.3 172.16.1...
17.07.2007 23:49:05 ICMP Typ... allowed Outbound ICMP 91.103.64.3 172.16.1...
17.07.2007 23:49:05 ICMP Typ... allowed Inbound ICMP 91.103.64.3 172.16.1...
17.07.2007 23:49:13 ICMP Typ... allowed Outbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:13 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:13 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:13 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:13 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:15 ICMP Typ... allowed Outbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:15 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
17.07.2007 23:49:15 ICMP Typ... allowed Inbound ICMP 91.103.64.141 172.16.1...
Actions...

Figure 91. Monitored data packets

Activity is only recorded if **Log event** is checked in the rule. It is unchecked by default in the packet filtering rules included with Kaspersky Anti-Virus for Windows Workstations.

The outcome of filtration (whether the packet was blocked), direction of the packet, the protocol, and other network connection settings for sending and receiving packets are indicated for each packet.

17.3.16. The *Established Connections* tab

All active network connections established on your computer at present are listed on the **Established connections** tab (see Figure 92). Here you will find the name of the application that initiated the connection, the protocol used, the direction of the connection (inbound or outbound), and connection settings (local and remote ports and IP addresses). You can also see how long a connection has been active and the volume of data sent and received. You can create or delete rules for connection. To do so, use the appropriate options on the context menu.

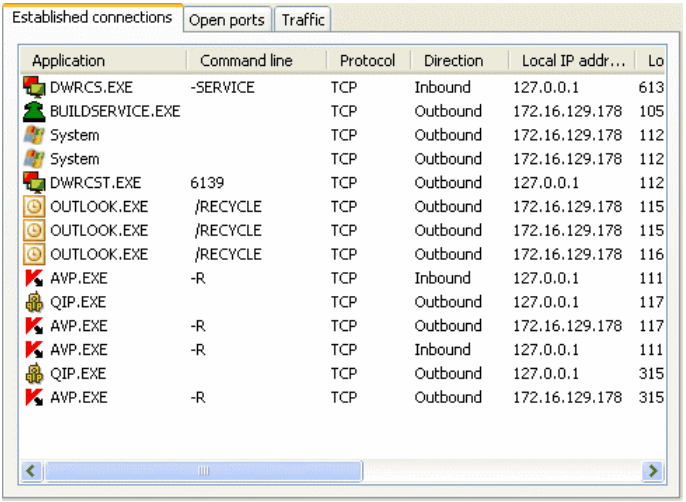

Established connections
Open ports
Traffic
Application
Command line
Protocol
Direction
Local IP addr...
Lo
DWRCS.EXE -SERVICE TCP Inbound 127.0.0.1 613
BUILDSERVICE.EXE TCP Outbound 172.16.129.178 105
System TCP Outbound 172.16.129.178 112
System TCP Outbound 172.16.129.178 112
DWRCST.EXE 6139 TCP Outbound 127.0.0.1 112
OUTLOOK.EXE /RECYCLE TCP Outbound 172.16.129.178 115
OUTLOOK.EXE /RECYCLE TCP Outbound 172.16.129.178 115
OUTLOOK.EXE /RECYCLE TCP Outbound 172.16.129.178 116
AVP.EXE -R TCP Inbound 127.0.0.1 111
QIP.EXE TCP Outbound 127.0.0.1 117
AVP.EXE -R TCP Outbound 172.16.129.178 117
AVP.EXE -R TCP Inbound 127.0.0.1 111
QIP.EXE TCP Outbound 127.0.0.1 315
AVP.EXE -R TCP Outbound 172.16.129.178 315

Figure 92. List of established connections

17.3.17. The *Open Ports* tab

All ports currently open on your computer for network connections are listed on the *Open ports* tab (see Figure 93). It lists the port number, data transfer protocol, name of the application that uses the port, and how long the port has been open for each port.

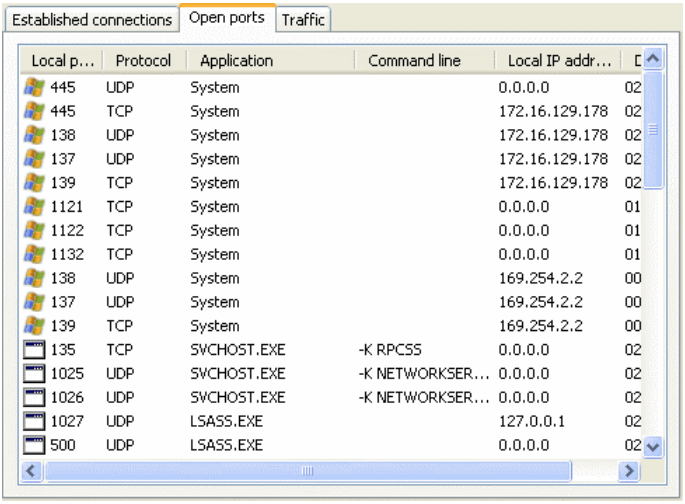

Established connections
Open ports
Traffic
Local p...
Protocol
Application
Command line
Local IP addr...
445 UDP System 0.0.0.0 02
445 TCP System 172.16.129.178 02
138 UDP System 172.16.129.178 02
137 UDP System 172.16.129.178 02
139 TCP System 172.16.129.178 02
1121 TCP System 0.0.0.0 01
1122 TCP System 0.0.0.0 01
1132 TCP System 0.0.0.0 01
138 UDP System 169.254.2.2 00
137 UDP System 169.254.2.2 00
139 TCP System 169.254.2.2 00
135 TCP SVCHOST.EXE -K RPCSS 0.0.0.0 02
1025 UDP SVCHOST.EXE -K NETWORKSER... 0.0.0.0 02
1026 UDP SVCHOST.EXE -K NETWORKSER... 0.0.0.0 02
1027 UDP LSASS.EXE 127.0.0.1 02
500 UDP LSASS.EXE 0.0.0.0 02

Figure 93. List of ports open on a computer

This information may be useful during virus outbreaks and network attacks if you know exactly which port is vulnerable. You can find out whether that port is open on your computer and take the necessary steps to protect your computer (for example, enabling Intrusion Detector, closing the vulnerable port, or creating a rule for it).

17.3.18. The *Traffic* tab

This tab (see Figure 94) holds information on all the inbound and outbound connections established between your computer and other computers, including web servers, email servers, etc. The following information is given for every connection: name and IP address of the host that the connection is with, and the amount of traffic sent and received.

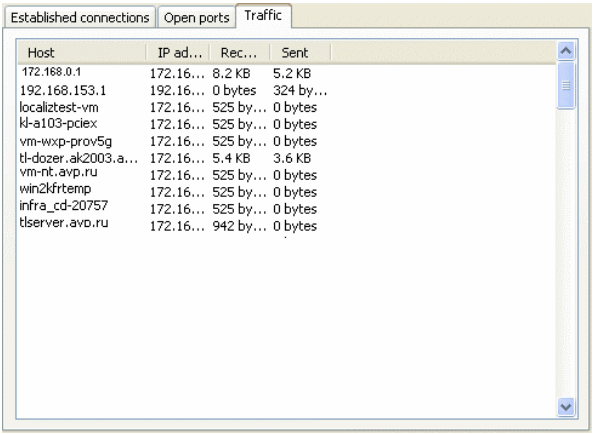

Established connections
Open ports
Traffic
Host
IP ad...
Rec...
Sent
172.168.0.1 172.16... 8.2 KB 5.2 KB
192.168.153.1 192.16... 0 bytes 324 by...
localiztest-vm 172.16... 525 by... 0 bytes
kl-a103-pciex 172.16... 525 by... 0 bytes
vm-wxp-prov5g 172.16... 525 by... 0 bytes
tl-dozer.ak2003.a... 172.16... 5.4 KB 3.6 KB
vm-nt.avp.ru 172.16... 525 by... 0 bytes
win2kfrtemp 172.16... 525 by... 0 bytes
infra_cd-20757 172.16... 525 by... 0 bytes
tlserver.avp.ru 172.16... 942 by... 0 bytes

Figure 94. Traffic on established network connections

17.4. General information about the program

You can view general information on the program in the **Service** section of the main window (see Figure 95).

All the information is broken into three sections:

- The program version, the date of the last update, and the number of threats known to date are displayed in the **Product info** box.
- Basic information on the operation system installed on your computer is shown in the **System info** box.
- Basic information about the license you purchased for Kaspersky Anti-Virus is contained in the **License info** box.

You will need all this information when you contact Kaspersky Lab Technical Support (see 17.6 on pg. 244).

Figure 95. Information on the program, the license, and the system it is installed on

17.5. Managing licenses

Kaspersky Anti-Virus for Windows Workstations needs a *license key* to operate. You are given the key when you buy the product and it gives you the right to use the program from the day you install the key.

Without a license key, unless a trial version of the application has been activated, Kaspersky Anti-Virus will run in one update mode. The program will not download any new updates.

If a trial version of the program has been activated, after the trial period expires, Kaspersky Anti-Virus will not run.

When a commercial license key expires, the program will continue working, except that you will not be able to update threat signatures. As before, you will be able to scan your computer for viruses and use the protection components, but only using the threat signatures that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your program license expires.

To avoid infecting your computer with new viruses, we recommend extending your Kaspersky Anti-Virus for Windows Workstations license. The program will notify you two weeks prior to the expiration of your license, and for the next two weeks it will display this message every time you open it.

To renew the license, you will need to purchase and install a new application license key or enter an application activation code. To do so:

Contact your product vendor and purchase an application license key or application code.

or:

Purchase a license key or an activation code directly from Kaspersky Lab by clicking Purchase License in the license key dialog (see Figure 96). Complete the appropriate form on the resulting webpage. Once payment is made, a link will be sent to the email address you entered in the order form. This link will enable you to download an application license key or obtain an activation code.

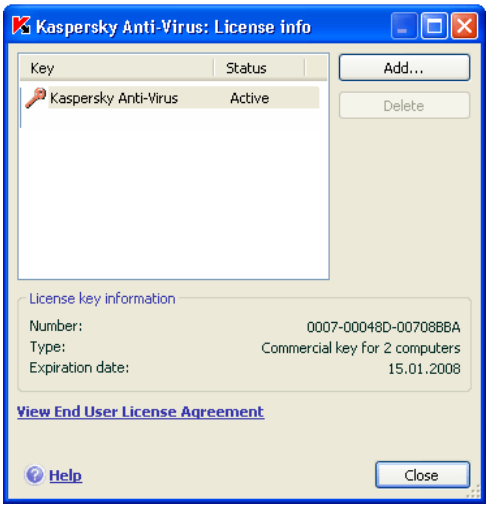


Figure 96. License information

Kaspersky Lab regularly has special pricing offers on license extensions for our products. Check for specials on the Kaspersky Lab website in the **Products → Sales and special offers** area.

Information on the current license key is available in the **License info** box of the **Service** section of the main application window. To go to the license manager

window, left-click anywhere in the box. In the window that opens (see Figure 96), you can view information on the current key, add a key, or delete one.

When you select a key from the list in the **License info** box, information will be displayed on the license number, type, and expiration date. To add a new license key, click **Add** and activate the application with the activation wizard. To delete a key from the list, press the **Delete** button.

To review the terms of the license agreement, click View End User License Agreement. To obtain a license through the web form on the Kaspersky Lab website, click Purchase license.

17.6. Technical Support

Kaspersky Anti-Virus for Windows Workstations provides you with a wide range of options for questions and problems related to program operation. They are all located in **Support** (see Figure 97) in the **Service** section.

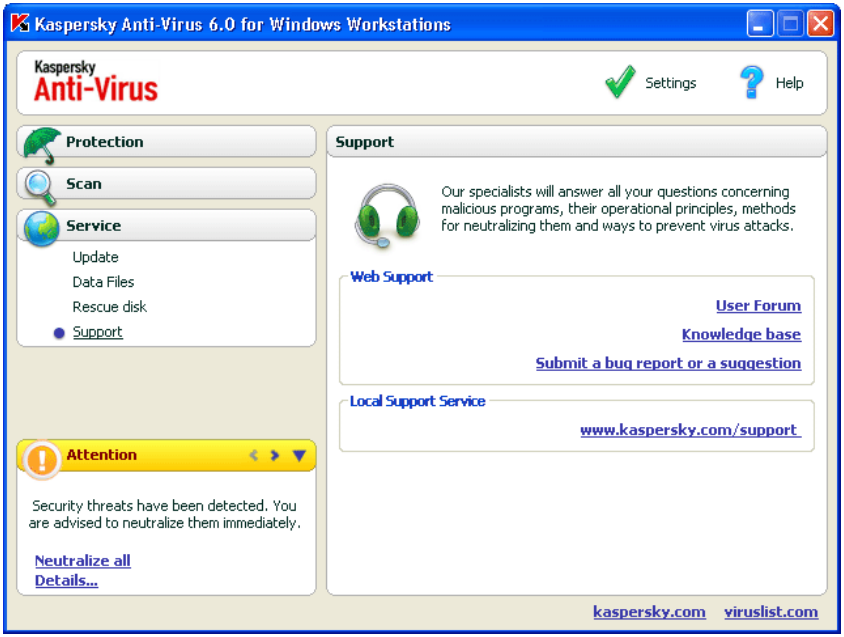


Figure 97. Technical support information

Depending on the problem, we provide several technical support services:

User forum. This resource is a dedicated section of the Kaspersky Lab website with questions, comments, and suggestions by program users. You can look through the basic topics of the forum and leave a comment yourself. You also might find the answer to your question.

To access this resource, use the User forum link.

Knowledge Base. This resource is also a dedicated section of the Kaspersky Lab website and contains Technical Support recommendations for using Kaspersky Lab software and answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

To obtain technical support online, click the Knowledge Base link.

Comments on program operation. This service is designed for posting comments on program operation or describing a problem that surfaced in program operation. You must fill out a special form on the company's website that describes the situation in detail. In order to best deal with the problem, Kaspersky Lab will need some information about your computer. You can describe the system configuration on your own or use the automatic information collector on your computer.

To go to the comment form, use the Submit a bug report or a suggestion link.

Technical support. If you need help with using Kaspersky Anti-Virus, click the link located in the **Local Support Service** box. The Kaspersky Lab website will then open with information about how to contact our specialists.

17.7. Creating a monitored port list

Protection components such as Mail Anti-Virus, Web Anti-Virus, Anti-Spy, and Anti-Spam monitor data streams that are transmitted using certain protocols and pass through certain open ports on your computer. Thus, for example, Mail Anti-Virus analyzes information transferred using SMTP protocol, and Web Anti-Virus analyzes information transferred using HTTP.

The standard list of ports that are usually used for transmitting email and HTTP traffic is included in the program package. You can add a new port or disable monitoring for a certain port, thereby disabling dangerous object detection for traffic passing through that port.

To edit the monitored port list, take the following steps:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking the Settings link in the main window.

2. Select **Network settings** in the **Service** section of the program settings tree.
3. In the right-hand part of the settings window, click **Port settings**.
4. Edit the list of the monitored ports in the window that opens (see Figure 98).

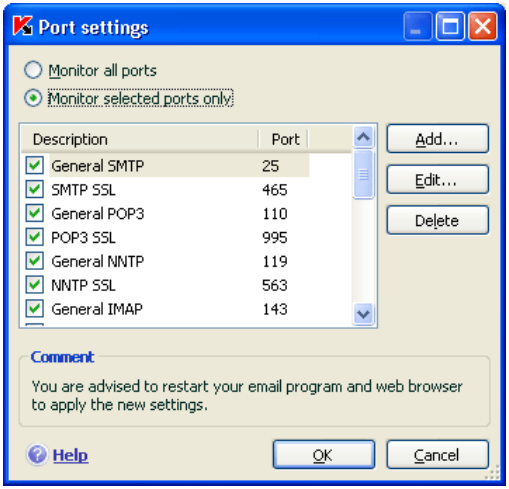


Figure 98. List of monitored ports

This window provides a list of ports monitored by Kaspersky Anti-Virus. To scan data streams enter on all open network ports, select the option **Monitor all ports**. To edit the list of monitored ports manually, select **Monitor selected ports only**.

We do not recommend selecting the **Monitor all ports** option when administering Kaspersky Anti-Virus 6.0 through Kaspersky Administration Kit if installed on a computer running Microsoft Windows 98. Otherwise problems may arise in accessing network resources and the Internet.

To add a new port to the monitored port list:

1. Click on the **Add** button in the **Port settings** window.
2. Enter the port number and a description of it in the appropriate fields in the **New Port** window.

For example, there might be a nonstandard port on your computer through which data is being exchanged with a remote computer using the HTTP protocol, which is monitored by Web Anti-Virus. To analyze this traffic for malicious code, you can add this port to a list of controlled ports.

When any of its components starts, Kaspersky Anti-Virus for Windows Workstations opens port 1110 as a listening port for all incoming connections. If that port is busy at the time, it selects 1111, 1112, etc. as a listening port.

If you use Kaspersky Anti-Virus for Windows Workstations and another company's firewall simultaneously, you must configure that firewall to allow the *avp.exe* process (the internal Kaspersky Anti-Virus for Windows Workstations process) access to all the ports listed above.

For example, say your firewall contains a rule for *iexplorer.exe* that allows that process to establish connections on port 80.

However, when Kaspersky Anti-Virus for Windows Workstations intercepts the connection query initiated by *iexplorer.exe* on port 80, it transfers it to *avp.exe*, which in turn attempts to establish a connection with the web page independently. If there is no allow rule for *avp.exe*, the firewall will block that query. The user will then be unable to access the webpage.

17.8. Checking encrypted connections

Connecting using SSL protocol protects data exchange through the Internet. SSL protocol can identify the parties exchanging data using electronic certificates, encode the data being transferred, and ensure their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus programs do not scan SSL traffic.

Kaspersky Anti-Virus 6.0 has the option of scanning SSL traffic for viruses. When an attempt is made to connect securely to a web resource, a notification will appear on screen (see Figure 99) prompting the user for action.

The notification contains information on the program initiating the secure connection, along with the remote address and port. The program asks you to decide whether that connection should be scanned for viruses:

- **Process** – scan traffic for viruses when connecting securely to the website.

  We recommend that you always scan SSL traffic if you are using a suspicious website or if an SSL data transfer begins when you go to the next page. It is quite likely that this is a sign of a malicious program being transferred over secure protocol.

- **Skip** – continue secure connection with the website without scanning traffic for viruses.

To apply the action selected in the future to all attempts to establish SSL connections, check **Apply to all**.

Traffic Monitor: training
Outgoing encrypted connection
Internet Explorer
Remote address: 10.64.0.7
Remote port: 3128
Scan encrypted connection
Apply to all
Process
Skip
Kaspersky Internet Security can scan this encrypted connection for viruses. Do you want this connection to be scanned?

Figure 99. Notification on SSL connection detection

To scan encrypted connections, Kaspersky Anti-Virus replaces the security certificate requested with a certificate it signs itself. In some cases, programs that are establishing connections will not accept this certificate, resulting in no connection being established. We recommend disabling SSL traffic scanning in the following cases:

- When connecting to a trusted web resource, such as your bank's web page, where you manage your personal account. In this case, it is important to receive confirmation of the authenticity of the bank's certificate.
- If the program establishing the connection checks the certificate of the website being accessed. For example, MSN Messenger checks the authenticity of the Microsoft Corporation digital signature when it establishes a connection with the server.

You can configure SSL scan settings on the **Encrypted connection** tab of the program settings window:

Check all encrypted connections – scan all traffic incoming on SSL protocol for viruses.

Prompt user when a new encrypted connection is detected – display a message prompting the user for action every time an SSL connection is established.

Do not check encrypted connections – do not scan traffic incoming on SSL protocol for viruses.

17.9. Configuring the Kaspersky Anti-Virus for Windows Workstations interface

Kaspersky Anti-Virus for Windows Workstations gives you the option of changing the appearance of the program by creating and using skins. You can also configure the use of active interface elements such as the system tray icon and popup messages.

To configure the program interface, take the following steps:

1. Open the Kaspersky Anti-Virus for Windows Workstations settings window by clicking the Settings link in the main window.
2. Select **Appearance** in the **Service** section of the program settings tree (see Figure 100).

In the right-hand part of the settings window, you can determine:

- Whether to display the Kaspersky Anti-Virus for Windows Workstations protection indicator when the operating system starts.

  This indicator by default appears in the upper right-hand corner of the screen when the program loads. It informs you that your computer is protected from all threat types. If you do not want to use the protection indicator, uncheck **Show icon above Microsoft Windows login window**.

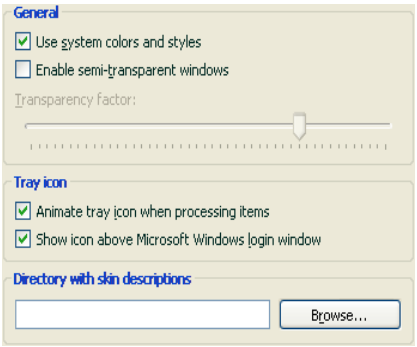


Figure 100. Configuring program appearance settings

- Whether to use animation in the system tray icon.

Depending on the program operation performed, the system tray icon changes. For example, if a script is being scanned, a small depiction of a script appears in the background of the icon, and if an email is being scanned, an envelope. By default, icon animation is enabled. If you want to turn off animation, uncheck **Animate tray icon when processing items**. Then the icon will only reflect the protection status of your computer: if protection is enabled, the icon is in color, and if protection is paused or disabled, the icon becomes gray.

- Degree of transparency of popup messages.

  All Kaspersky Anti-Virus for Windows Workstations operations that must immediately reach you or require you to make a decision are presented as popup messages above the system tray icon. The message windows are transparent so as not to interfere with your work. If you move the cursor over the message, the transparency disappears. You can change the degree of transparency of such messages. To do so, adjust the **Transparency factor** scale to the desired position. To remove message transparency, uncheck **Enable semi-transparent windows**.

  This feature is unavailable under Windows 98/NT 4.0/ME.

- Use your own skins for the program interface.

  All the colors, fonts, icons, and texts used in the Kaspersky Anti-Virus for Windows Workstations interface can be changed. You can create your own graphics for the program or can localize it in another language. To use a skin, specify the directory with its settings in the **Directory with skin descriptions** field. Use the **Browse** button to select the directory.

  By default, the system colors and styles are used in the program's skin. You can remove them by deselecting **Use system colors and styles**. Then the styles that you specify in the screen theme settings will be used.

Note that changes to Kaspersky Anti-Virus for Windows Workstations interface settings are not saved if you restore default operation settings or uninstall the program.

17.10. Rescue Disk

Kaspersky Anti-Virus for Windows Workstations has a tool for creating a rescue disk.

The rescue disk is designed to restore system functionality after a virus attack that has damaged system files and made the operating system impossible to start. This disk includes:

- Microsoft Windows XP Service Pack 2 system files
- A set of operating system diagnostic utilities
- Kaspersky Anti-Virus for Windows Workstations program files
- Files containing threat signatures

To create a rescue disk:

1. Open the program's main window and select **Rescue disk** in the **Service** section.
2. Click the **Start Wizard** button to begin creating the disk.

A Rescue Disk is designed for the computer that it was created on. Using the disk on other computers could lead to unforeseeable consequences, since it contains information about the parameters of a specific computer (info on boot sectors, for example).

You can only create a rescue disk under Windows XP and Microsoft Windows Vista. You cannot create a rescue disk on computers running Microsoft Windows XP Professional x64 Edition or Microsoft Windows Vista x64.

17.10.1. Creating a rescue disk

Warning! You will need the Microsoft Windows XP Service Pack 2 installation disk to create a rescue disk.

You need the program **PE Builder** to create the Rescue Disk.

You must install these PE Builder on your computer beforehand to create a disk with it.

A special Wizard walks you through the creation of a rescue disk. It consists of a series of windows/steps which you can navigate using the **Back** and **Next** buttons. You can complete the Wizard by clicking **Finished**. The **Cancel** button will stop the Wizard at any point.

Step 1. Getting ready to write the disk

To create a rescue disk, specify the path to the following folders:

- PE Builder program folder
- Folder where rescue disk files will be saved before burning the CD

If you are not creating a disk for the first time, this folder will already contain a set of files made the last time. To use files saved previously, check the corresponding box.

> Note that a previous version of the rescue disk files will contain outdated threat signatures. To optimally analyze the computer for viruses and to restore the system, we recommend updating threat signatures and creating a new version of the rescue disk.

- The Microsoft Windows XP Service Pack 2 installation CD

To create a rescue disk that can boot the operating system on a remote computer and scan and processing malicious code using Kaspersky Anti-Virus, check **Allow remote administration of computer being scanned**.

Note that to use this feature, the remote computer must support Intel® vPRO™ or Intel® Active Management Technology (iAMT). These technologies allow administrators to work with all computers connected to the network remotely, including those that are turned off and those whose operating systems or hard drives are not functioning.

After entering the paths to the folders required, click **Next**. PE Builder will start up and the rescue disk creation process will begin. Wait until the process is complete. This could take several minutes.

Step 2. Creating an .iso file

After PE Builder has completed creating the rescue disk files, a **Create .iso file** window will open.

The .iso file is a CD image of the disk, saved as an archive. The majority of CD burning programs correctly recognize .iso files (Nero, for example).

If this is not the first time that you have created a rescue disk, you can select the .iso file from the previous disk. To do so, select **Existing .iso file**.

Step 3. Burning the disk

This Wizard window will ask you to choose whether to burn the rescue disk files to CD now or later.

If you chose to burn the disk right away, specify whether you want to format the CD before burning. To do so, check the corresponding box. You only have this option if you are using a CD-RW.

The CD will start burning when you click the **Next** button. Wait until the process is complete. This could take several minutes.

Step 4. Finishing creating a rescue disk

This Wizard window informs you that you have successfully created a rescue disk.

17.10.2. Using the rescue disk

Note that Kaspersky Anti-Virus only works in system rescue mode if the main window is opened. When you close the main window, the program will close.

Bart PE, the default program, does not support .chm files or Internet browsers, so you will not be able to view Kaspersky Anti-Virus Help or links in the program interface while in Rescue Mode.

If a situation arises when a virus attack makes it impossible to load the operating system, take the following steps:

1. Create an emergency boot disk by using Kaspersky Anti-Virus for Windows Workstations on an uninfected computer.
2. Insert the rescue disk in the disk drive of the infected computer and restart. Microsoft Windows XP SP2 will start with the Bart PE interface. Bart PE has built-in network support for using your LAN. When the program starts, it will ask you if you want to enable it. You should enable network support if you plan to update threat signatures from the LAN before scanning your computer. If you do not need to update, cancel network support.
3. To open Kaspersky Anti-Virus, click **Start→Programs→Kaspersky Anti-Virus 6.0 for Windows Workstations →Start**.

   The Kaspersky Anti-Virus for Windows Workstations main window will open. In system rescue mode, you can only access virus scans and threat signature updates from the LAN (if you have enabled network support in Bart PE).
4. Start the virus scan.

Note that threat signatures from the date that the rescue disk is created are used by default. For this reason, we recommend updating threat signatures before starting the scan.

It should also be noted that the application will only use the updated Threat Signatures during the current session with the rescue disk, prior to restarting your computer.

Warning!

If infected or potentially infected objects were detected when you scanned the computer, and they were processed and then moved to Quarantine or Backup Storage, we recommend completing processing those objects during the current session with a rescue disk.

Otherwise, these objects will be lost when you restart your computer.

17.11. Using additional services

Kaspersky Anti-Virus for Windows Workstations provides you with the following advanced features:

- Notifications of certain events that occur in the program.
- Kaspersky Anti-Virus for Windows Workstations Self-Defense against modules being disabled, deleted, or edited, as well as password protection for the program.
- Resolving conflicts with Kaspersky Anti-Virus 6.0 when using other applications.

To configure these features:

1. Open the program setup window with the Settings link in the main window.
2. Select **Service** from the settings tree.

In the right hand part of the screen you can define whether to use additional features in program operation.

17.11.1. Kaspersky Anti-Virus for Windows Workstations event notifications

Different kinds of events occur in Kaspersky Anti-Virus for Windows Workstations. They can be of an informative nature or contain important information. For example, an event can inform you that the program has updated successfully, or can record an error in a component that must be immediately eliminated.

To receive updates on Kaspersky Anti-Virus for Windows Workstations operation, you can use the notification feature.

Notices can be delivered in several ways:

- Popup messages above the program icon in the system tray
- Sound messages
- Emails
- Recording information in the event log

To use this feature, you must:

1. Check **Enable notifications** in the **Interaction with user** box (see Figure 101).

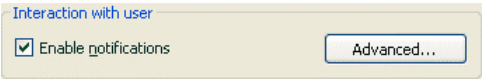


Figure 101. Enabling notifications

2. Define the event types from Kaspersky Anti-Virus for Windows Workstations for which you want notifications, and the notification delivery method (see 17.11.1.1 on pg. 255).
3. Configure email notification delivery settings, if that is the notification method that is being used (see 17.11.1.2 on pg. 257).

17.11.1.1. Types of events and notification delivery methods

During Kaspersky Anti-Virus for Windows Workstations operation, the following kinds of events arise:

Critical notifications are events of a critical importance. Notifications are highly recommended, since they point to problems in program operation or vulnerabilities in protection on your computer. For example, *threat signatures corrupt* or *license expired*.

Error notifications – events that lead to the application not working. For example, no license or threat signatures.

Important notifications are events that must be investigated, since they reflect important situations in the operation of the program. For example, *protection disabled* or *computer has not been scanned for viruses for a long time.*

Minor notifications are reference-type messages which generally do not contain important information. For example, *all dangerous objects disinfected*.

To specify which events the program should notify you of and how:

1. Click the Settings link in the program's main window.
2. In the program settings window, select **Service**, check **Enable notifications**, and edit detailed settings by clicking the **Settings** button.

You can configure the following notification methods for the events listed above in the **Notification Settings** window that opens (see Figure 102):

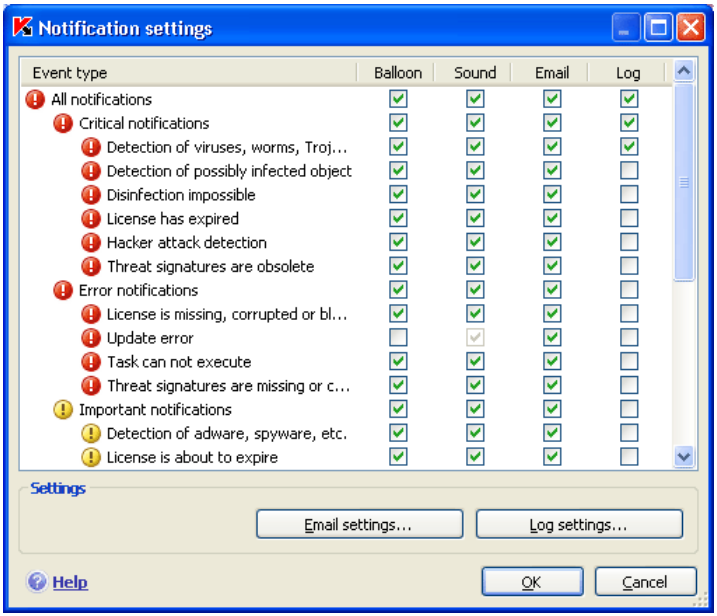


Figure 102. Program events and event notification methods

- *Popup messages* above the program icon in the system tray that contain an informative message on the event that occurred.

  To use this notification type, check in the **Balloon** section across from the event about which you want to be informed.

- *Sound notification*

  If you want this notice to be accompanied by a sound file, check **Sound** across from the event.

- *Email notification*

To use this type of notice, check the **Email** column across from the event about which you want to be informed, and configure settings for sending notices (see 17.11.1.2 on pg. 257).

- *Recording information in the event log*

  To record information in the log about events that occur, check in the **Log** column and configure event log settings (see 17.11.1.3 on pg. 258).

17.11.1.2. Configuring email notification

After you have selected the events (see 17.11.1.1 on pg. 255) about which you wish to receive email notifications, you must set up notification delivery. To do so:

1. Open the program setup window with the Settings link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** box on the right-hand part of the screen.
4. On the **Notification settings** tab (see Figure 102), select the checkbox in the **E-mail** graph for events that should trigger an e-mail message.
5. In the window that opens when you click **Notification settings**, configure the following settings for sending e-mail notifications:
   - Assign the sending notification setting for **From: Email address**.
   - Specify the email address to which notices will be sent in **To: Email address**.
   - Assign a email notification delivery method in the **Send mode**. If you want the program to send email as soon as the event occurs, select **Immediately when event occurs**. For notifications about events within a certain period of time, fill out the schedule for sending informative emails by click **Edit**. Daily notices are the default.

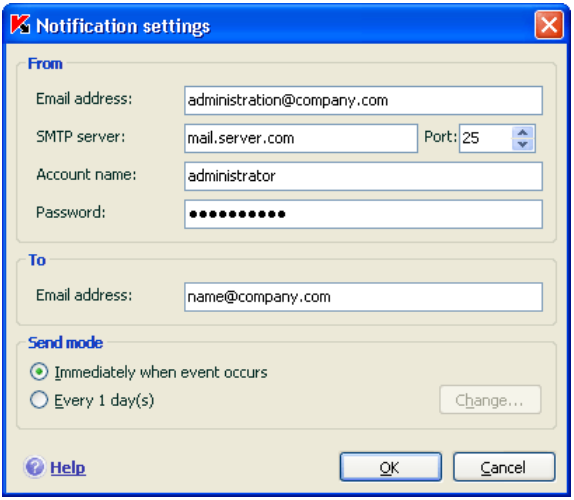


Figure 103. Configuring email notification settings

17.11.1.3. Configuring event log settings

To configure event log settings:

1. Open the application settings window with the Settings link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** section of the right-hand part of the screen.

In the **Notification Settings** window, select the option of logging information for an event and click the **Log Settings** button.

Kaspersky Anti-Virus has the option of recording information about events that arise while the program is running, either in the MS Windows general event log (**Application**) or in a dedicated Kaspersky Anti-Virus event log (**Kaspersky Event Log**).

Under Microsoft Windows 98/ME, you cannot record to the event log. Under Microsoft Windows NT 4.0, you cannot record to **Kaspersky Event Log**.

These limitations are because of the features of these operating systems.

Logs can be viewed in the MS Event Viewer, which you can open by going to **Start → Settings → Control Panel → Administration → View Events**.

17.11.2. Self-Defense and access restriction

Kaspersky Anti-Virus for Windows Workstations ensures your computer's security against malicious programs, and because of that it can itself be the target of malicious programs that try to block it or delete it from the computer.

Moreover, several people may be using the same computer, all with varying levels of computer literacy. Leaving access to the program and its settings open could dramatically lower the security of the computer as a whole.

To ensure the stability of your computer's security system, Self-Defense, remote access defense, and password protection mechanisms have been added to the program.

If you are running Kaspersky Anti-Virus under Microsoft Windows 98/ME, the application self-defense feature is not available.

On computers running 64-bit operating systems and Microsoft Windows Vista, self-defense is only available for preventing the program's own files on local drives and system registry records from being modified or deleted.

To enable Self-Defense:

1. Open the program settings window with the Settings link in the main window.
2. Select **Service** from the settings tree.
3. Make the following configurations in the **Self-Defense** box (see Figure 104):

☑ **Enable Self-Defense**. If this box is checked, the program will protect its own files, processes in memory, and entries in the system registry from being deleted or modified.

☑ **Disable external service control**. If this box is checked, any remote administration program attempting to use the program will be blocked.

If any of the actions listed are attempted, a message will appear over the program icon in the system tray (if the notification service has not been disabled by the user).

Figure 104. Configuring program defense

To password-protect the program, check **Enable password protection**. Click on the **Settings** button to open the **Password Protection** window, and enter the password and area that the access restriction will cover (see Figure 105). You can block any program operations, except notifications for dangerous object detection, or prevent any of the following actions from being performed:

- Change of program performance settings
- Close Kaspersky Anti-Virus for Windows Workstations
- Disable or pause protection on your computer

Each of these actions lowers the level of protection on your computer, so try to establish which of the users on your computer you trust to take such actions.

Now whenever any user on your computer attempts to perform the actions you selected, the program will request a password.

Figure 105. Program password protection settings

17.11.3. Resolving conflicts with other applications

In some cases, Kaspersky Anti-Virus may cause conflicts with other applications installed on a computer. This is because those programs have built-in self-defense mechanisms that turn on when Kaspersky Anti-Virus attempts to inspect them. These applications include the Authentica plug-in for Acrobat Reader, which verifies access to .pdf files, Oxygen Phone Manager II, and some computer games that have digital rights management tools.

To fix this problem, check **Compatibility mode for programs using self-protection methods** in the **Service** section of the application settings window. You must restart your operating system for this change to take effect.

If Kaspersky Anti-Virus is installed on the computer running Microsoft Windows Vista or Microsoft Windows Vista x64 resolving problems of compatibility with other applications is unavailable.

However, note that if you select the checkbox, some Kaspersky Anti-Virus features, specifically Office Guard and Anti-Dialer, will not work. If you enable either of these components, compatibility with application self-dense will be disabled automatically. Once enabled, these components will only begin running after you restart the application.

17.12. Importing and exporting Kaspersky Anti-Virus for Windows Workstations settings

Kaspersky Anti-Virus for Windows Workstations allows you to import and export its own settings.

This feature is useful when, for example, the program is installed both on your home computer and in your office. You can configure the program the way you want it at home, save those settings on a disk, and using the import feature, load them on your computer at work. The settings are saved in a special configuration file.

To export the current program settings:

1. Open the Kaspersky Anti-Virus for Windows Workstations main window.
2. Select the **Service** section and click Settings.

3. Click the **Save** button in the **Configuration manager** section.
4. Enter a name for the configuration file and select a save destination.

To import settings from a configuration file:

1. Open the Kaspersky Anti-Virus for Windows Workstations main window.
2. Select the **Service** section and click Settings.
3. Click the **Load** button and select the file from which you want to import Kaspersky Anti-Virus for Windows Workstations settings.

17.13. Resetting to default settings

It is always possible to return to the default program settings, which are considered the optimum and are recommended by Kaspersky Lab. This can be done using the Setup Wizard.

To reset protection settings:

1. Select the **Service** section and click Settings to go to the program configuration window.
2. Click the **Reset** button in the **Configuration manager** section.

The window that opens asks you to define which settings should be restored to their default values.

The window lists the program components whose settings were changed by the user, or that the program accumulated through training (Anti-Hacker or Anti-Spam). If special settings were created for any of the components, they will also be shown on the list.

Examples of special settings would be white and black lists of phrases and addresses used by Anti-Spam, trusted address lists and trusted ISP telephone number lists used by Web Anti-Virus and Anti-Spy, exclusion rules created program components, packet filtering and application rules for Anti-Hacker, and application rules for Proactive Defense

These lists are usually populated gradually through extended use of the program, based on individual tasks and security requirements, and usually take some time to create. Therefore, you are advised to save them before you reset program settings.

The program saves all the custom settings on the list by default (they are unchecked). If you do not need to save one of the settings, check the box next to it.

After you have finished configuring the settings, click the **Next** button. Initial Setup Wizard will open (see 3.2 pg. 36). Follow its instructions.

After you are finished with the Setup Wizard, the **Recommended** security level will be set for all components, except for the settings that you decided to keep. In addition, settings that you configured with the Setup Wizard will also be applied.

CHAPTER 18. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT

You can use Kaspersky Anti-Virus from the command prompt. You can execute the following operations:

- Starting, stopping, pausing and resuming the activity of application components
- Starting, stopping, pausing and resuming virus scans
- Obtaining information on the current status of components, tasks and statistics on them
- Scanning selected objects
- Updating threat signatures and program modules
- Accessing Help for command prompt syntax
- Accessing Help for command syntax

The command prompt syntax is:

```
avp.com <command> [settings]
```

> You must access the program from the command prompt from the program installation folder or by specifying the full path to avp.com.

The following may be used as **<commands>**:

ADDKEY	Activates application using a license key file (command can only be executed if the password assigned through the program interface is entered)
ACTIVATE	Activates the application online using an activation code
START	Starts a component or a task
PAUSE	Pauses a component or a task (command can only be executed if the password assigned through the program interface is entered)

RESUME	Resumes a component or a task
STOP	Stops a component or a task (command can only be executed if the password assigned through the program interface is entered)
STATUS	Displays the current component or task status on screen
STATISTICS	Displays statistics for the component or task on screen
HELP	Help with command syntax and the list of commands
SCAN	Scans objects for viruses
UPDATE	Begins program update
ROLLBACK	Rolls back to the last program update made (command can only be executed if the password assigned through the program interface is entered)
EXIT	Closes the program (you can only execute this command with the password assigned in the program interface)
IMPORT	Import Kaspersky Anti-Virus for Windows Workstations settings (command can only be executed if the password assigned through the program interface is entered)
EXPORT	Export Kaspersky Anti-Virus for Windows Workstations settings

Each command uses its own settings specific to that particular Kaspersky Anti-Virus for Windows Workstations component.

18.1. Activating the application

There are two ways to activate the application:

- online using an activation code (ACTIVATE command)
- using a license key file (ADDKEY command).

Command syntax:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Parameter description:

<file_name>	Name of the license key file with the extension *.key*.
<activation_code>	Application activation code provided at purchase.
<password>	Password for accessing Kaspersky Anti-Virus assigned in the application interface.
Note that you cannot execute this command without entering the password.	

Example:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

18.2. Managing program components and tasks

Command syntax:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parameters:

<command>	Kaspersky Anti-Virus provides task and component management from the command line using the commands below: **START** – start real-time security component or task. **STOP** – stop real-time security component or task. **PAUSE** – pause real-time security component or task.

	RESUME – resume real-time security component or task. **STATUS** – display current real-time security component or task status. **STATISTICS** – display current real-time security component or task runtime statistics. Please note that PAUSE and STOP are password protected.
<profile|task_name>	The **<profile>** parameter may be assigned any real-time application security component or component module, on-demand scan task, or update as value (standard values used by the application are shown below). Valid values for the **<task_name>** parameter may include the name of any user-defined on-demand scan task or update.
<your_password>	Kaspersky Anti-Virus password set through the program interface.
/R[A]:<report_file>	**R:<report_file>**: log important events only. **/RA:<report_file>**: log all events. An absolute or a relative path to a file may be used. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

One of the following values is assigned to **<profile>**:

RTP	All protection components The command avp.com START RTP starts all real-time protection components if protection is fully disabled (see 6.1.2 on pg. 68) or paused (see 6.1.1 on pg. 67). This command will also start any real-time protection components that were paused using the ❚❚ button from the graphic user interface or the PAUSE command from the command prompt. If the component was disabled using the ■ button from the graphic user interface or the STOP

	command from the command prompt, the command avp.com START RTP will not start it. In order to start it, you must execute the command avp.com START <profile>, with the value for the specific protection component entered for <profile>. For example, avp.com START FM.
FM	File Anti-Virus
EM	Mail Anti-Virus
WM	Web Anti-Virus Values for Web Anti-Virus subcomponents: **httpscan** – scans http traffic **sc** – scans scripts
BM	Proactive Defense Values for Proactive Defense subcomponents: **og** – scans Microsoft Office macros **pdm** – application activity analysis
ASPY	Anti-Spy Values for Anti-Spy subcomponents: **AdBlocker** – AdBlocker **antidial** – Anti-Dialer **antiphishing** – Anti-Phishing **popupchk** – Popup Blocker
AH	Anti-Hacker Values for Anti-Hacker subcomponents: **fw** – Firewall **ids** – Intrusion Detection System
AS	Anti-Spam

UPDATER	Updater
RetranslationCfg	Update distribution to a local source
Rollback	Rolls back to the previous update
SCAN_OBJECTS	Virus scan task
SCAN_MY_COMPUTER	My Computer task
SCAN_CRITICAL_AREAS	Critical Areas task
SCAN_STARTUP	Startup Objects task
SCAN_QUARANTINE	Scans quarantined objects
Components and tasks started from the command prompt are run with the settings configured with the program interface.	

Examples:

To enable File Anti-Virus, type this at the command prompt:

```
avp.com START FM
```

To view the current status of Proactive Defense on your computer, type the following text at the command prompt:

```
avp.com STATUS BM
```

To stop a My Computer scan task from the command prompt, enter:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

18.3. Anti-virus scans

The syntax for starting a virus scan of a certain area, and processing malicious objects, from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

To scan objects, you can also start one of the tasks created in Kaspersky Anti-Virus for Windows Workstations from the command prompt (see 18.1 on pg. 265). The task will be run with the settings specified in the program interface.

Parameter description.

<table>
<tr><td colspan="2"><object scanned> - this parameter gives the list of objects that will be scanned for malicious code.
It can include several values from the following list, separated by spaces.</td></tr>
<tr><td><files></td><td>List of paths to the files and/or folders to be scanned. You can enter absolute or relative paths. Items in the list are separated by a space.
Notes:
If the object name contains a space, it must be placed in quotation marks
If you select a specific folder, all the files in it are scanned.</td></tr>
<tr><td>/MEMORY</td><td>System memory objects</td></tr>
<tr><td>/STARTUP</td><td>Startup objects</td></tr>
<tr><td>/MAIL</td><td>Email databases</td></tr>
<tr><td>/REMDRIVES</td><td>All removable media drives</td></tr>
<tr><td>/FIXDRIVES</td><td>All internal drives</td></tr>
<tr><td>/NETDRIVES</td><td>All network drives</td></tr>
<tr><td>/QUARANTINE</td><td>Quarantined objects</td></tr>
<tr><td>/ALL</td><td>Complete scan</td></tr>
<tr><td>/@:<filelist.lst></td><td>Path to a file containing a list of objects and folders to be included in the scan. The file should be in a text format and each scan object must start a new line.
You can enter an absolute or relative path to the file. The path must be placed in quotation marks if it contains a space.</td></tr>
<tr><td colspan="2"><action> - this parameter sets responses to malicious objects detected during the scan. If this parameter is not defined, the default value is /i8.</td></tr>
</table>

/i0	take no action on the object; simply record information about it in the report.
/i1	Treat infected objects, and if disinfection fails, skip
/i2	Treat infected objects, and if disinfection fails, delete. Exceptions: do not delete infected objects from compound objects; delete compound objects with executable headers, i.e. sfx archives (default).
/i3	Treat infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted.
/i4	Delete infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted.
/i8	Prompt the user for action if an infected object is detected.
/i9	Prompt the user for action at the end of the scan.
<file types> - this parameter defines the file types that will be subject to the anti-virus scan. If this parameter is not defined, the default value is /fi.	
/fe	Scan only potentially infected files by extension
/fi	Scan only potentially infected files by contents (default)
/fa	Scan all files
<exclusions> - this parameter defines objects that are excluded from the scan. It can include several values from the list provided, separated by spaces.	
-e:a	Do not scan archives
-e:b	Do not scan email databases

-e:m	Do not scan plain text emails
-e:<filemask>	Do not scan objects by mask
-e:<seconds>	Skip objects that are scanned for longer that the time specified in the **<seconds>** parameter.
-es:<size>	Skip files larger (in MB) than the value assigned by **<size>**.
<configuration file> - defines the path to the configuration file that contains the program settings for the scan. The configuration file is a text file that contains a group of command prompt settings for antivirus scans. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the Kaspersky Anti-Virus for Windows Workstations interface are used.	
/C:<file_name>	Use the settings values assigned in the configuration file **<file_name>**
<report settings> - this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.	
/R:<report_file>	Only log important events in this file
/RA:<report_file>	Log all events in this file
<Advanced settings> – settings that define use of anti-virus scanning technologies.	
/iChecker=<on|off>	Enable/ disable iChecker
/iSwift=<on|off>	Enable/ disable iSwift

Examples:

Start a scan of RAM, Startup programs, email databases, the directories **My Documents** *and* **Program Files***, and the file* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Pause scan of selected objects and start full computer scan, then continue to scan for viruses within the selected objects:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Scan RAM and the objects listed in the file ***object2scan.txt****. Use the configuration file* ***scan_setting.txt****. After the scan, generate a report in which all events are recorded:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

18.4. Program updates

The syntax for updating Kaspersky Anti-Virus for Windows Workstations program modules and threat signatures from the command prompt is as follows:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP=<on|off>]
```

Parameter description:

<update_source>	HTTP or FTP server or network directory for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If no path is specified, an update source will be copied from the application's update settings.

/R[A]:<report_file>	**/R:<report_file>** – only log important events in the report. **/R[A]:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.
/C:<file_name>	Path to the configuration file with the settings for program updates. The configuration file is a text file that contains a group of command prompt settings for updating the program. You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the Kaspersky Anti-Virus for Windows Workstations interface are used.
/APP=<on|off>	Enable / Disable application module updates

Examples:

Update threat signatures and record all events in the report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update the Kaspersky Anti-Virus for Windows Workstations program modules by using the settings in the configuration file **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

18.5. Rollback settings

Command syntax:

```
ROLLBACK
[/R[A]:<report_file>][/password=<your_password>]
```

/R[A]:<report_file>	**/R:<report_file>** – only log important events in the report. **/R[A]:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.
<your_password>	Password for accessing Kaspersky Anti-Virus assigned in the application interface.
Note that this command will not be accepted without a password.	

Example:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<your_password>
```

18.6. Exporting settings

Command syntax:

```
avp.com EXPORT <profile> <file_name>
```

Parameter description:

<profile>	Component or task with the settings being exported. You can use any value for **<profile>** that is listed in 18.2 on pg. 266.
<filename>	The configuration file can be saved as a text file. To do so, specify the *.txt* extension in the file name. You can also save the file in any binary format. The configuration file is saved in binary format (*.dat*), unless another format is specified or if the format is not assigned, and it can be used later to import application settings on other computers. The configuration file can be saved as a text file. To do so, specify the *.txt* extension in the file name. Note that protection settings cannot be imported from a text file. This file can only be used to specify the main settings for program operation.

Example:

```
avp.com EXPORT c:\settings.dat
```

18.7. Importing settings

Command syntax:

```
avp.com IMPORT <filename> [/password=<your_password>]
```

<filename>	The configuration file can be saved as a text file. To do so, specify the *.dat* extension in the file name. Settings can only be imported from binary files. If you install the program in hidden mode from the command prompt or with Group Policy Object Editor, the name on the configuration file must be *install.cfg*. Otherwise the program will not recognize it.
<your_password>	Kaspersky Anti-Virus password assigned in the program interface.
Note that this command will not be accepted without a password.	

Example:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

18.8. Starting the program

Command syntax:

```
avp.com
```

18.9. Stopping the program

Command syntax:

```
avp.com EXIT /password=<your_password>
```

<your_password>	Kaspersky Anti-Virus for Windows Workstations password assigned in the program interface.

Note that this command will not be accepted without a password.

Note that you cannot execute this command without entering the password.

18.10. Obtaining a Trace File

A trace file may be required in the event of application runtime issues for Technical Support specialists to perform more focused troubleshooting.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

[on|off]	Enable/Disable trace file generation.
[file]	Obtain a trace and save to file.
<trace_level>	This parameter may be assigned numeric values ranging from 0 (lowest level, critical events only) to 700 (highest level, all events). When a request is sent to Technical Support, a specialist must specify the required trace level. If not specified, the recommended level is 500.
Caution! Trace file generation should be enabled to troubleshoot a specific issue only. Keeping the trace functionality active at all times may reduce computer performance and cause the hard drive to become full.	

Examples:

Disable trace:

```
avp.com TRACE file off
```

Generate a trace file for Technical Support at maximum trace level of 500:

```
avp.com TRACE file on 500
```

18.11. Viewing Help

This command is available for viewing Help on command prompt syntax:

```
avp.com [ /? | HELP ]
```

To get help on the syntax of a specific command, you can use one of the following commands:

```
avp.com <command> /?
avp.com HELP <command>
```

18.12. Return codes from the command line interface

This section contains a list of return codes from the command line. The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

General return codes	
0	Operation completed successfully
1	Invalid setting value
2	Unknown error
3	Task completion error
4	Task canceled
Anti-virus scan task return codes	
101	All dangerous objects processed
102	Dangerous objects detected

CHAPTER 19. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM

You can uninstall the application in the following ways:

- Using the application's Setup Wizard (see 19.2 on pg. 281)
- From the command prompt (see 19.2 on pg. 281)
- Using Kaspersky Administration Kit (see Kaspersky Administration Kit Implementation Guide)
- Using Microsoft Windows Server 2000/2003 group domain policies (see 3.4.3 on pg. 46).

19.1. Modifying, repairing, and removing the program using Installation Wizard

You may find it necessary to repair the program if you detect errors in its operation after incorrect configuration or file corruption.

Modifying the program can install missing Kaspersky Anti-Virus for Windows Workstations components and delete unwanted ones.

To repair or modify Kaspersky Anti-Virus for Windows Workstations missing components or delete the program:

1. Exit the program. To do so, left-click on the program icon in the system tray and select **Exit** from the context menu.
2. Insert the installation CD into the CD-ROM drive, if you used one to install the program. If you installed Kaspersky Anti-Virus for Windows Workstations from a different source (public access folder, folder on the hard drive, etc.), make sure that the installer package is in the folder and that you have access to it.
3. Select **Start → Programs → Kaspersky Anti-Virus 6.0 for Windows Workstations → Modify, Repair, or Remove**.

An installation wizard then will open for the program. Let's take a closer took at the steps of repairing, modifying, or deleting the program.

Step 1. Installation Welcome window

If you take all the steps described above necessary to repair or modify the program, the Kaspersky Anti-Virus for Windows Workstations installation welcome window will appear. To continue, click the **Next** button.

Step 2. Selecting an operation

At this stage, you select which operation you want to run. You can modify the program components, repair the installed components, remove components or remove the entire program. To execute the operation you need, click the appropriate button. The program's response depends on the operation you select.

Modifying the program is like custom program installation (see Step 7. on pg. 34)where you can specify which components you want to install, and which you want to delete.

Repairing the program depends on the program components installed. The files will be repaired for all components that are installed and the Recommended security level will be set for each of them.

If you remove the program, you can select which data created and used by the program you want to save on your computer. To delete all Kaspersky Anti-Virus for Windows Workstations data, select **Complete uninstall**. To save data, select **Save application objects** and specify which objects not to delete from this list:

- *Activation data* – license key file necessary for the application to operate.
- *Threat signatures* – complete set of signatures of dangerous programs, virus, and other threats current as of the last update.
- *Anti-Spam base* – database used to detect junk email. This database contains detailed information on what email is spam and what is not.
- *Backup files* – backup copies of deleted or disinfected objects. You are advised to save these, in case they can be restored later.
- *Quarantine files* – files that are potentially infected by viruses or modifications of them. These files contain code that is similar to code of a known virus but it is difficult to determine if they are malicious. You are advised to save them, since they could actually not be infected, or they could be disinfected after the threat signatures are updated.

- *Application settings* – configurations for all program components.
- *iSwift data* – database with information on objects scanned on NTFS file systems, which can increase scan speed. When it uses this database, Kaspersky Anti-Virus for Windows Workstations only scans the files that have been modified since the last scan.

> Warning!
>
> If a long period of time elapses between uninstalling one version of Kaspersky Anti-Virus for Windows Workstations and installing another, you are advised not to use the *iSwift* database from a previous installation. A dangerous program could penetrate the computer during this period and its effects would not be detected by the database, which could lead to an infection.

To start the operation selected, click the **Next** button. The program will begin copying the necessary files to your computer or deleting the selected components and data.

Step 3. Completing program modification, repair, or removal

The modification, repair, or removal process will be displayed on screen, after which you will be informed of its completion.

Removing the program generally requires you to restart your computer, since this is necessary to account for modifications to your system. The program will ask if you want to restart your computer. Click **Yes** to restart right away. To restart your computer later, click **No**.

19.2. Uninstalling the program from the command prompt

To uninstall Kaspersky Anti-Virus 6.0 for Windows Workstations from the command prompt, enter:

```
msiexec /x <package_name>
```

The Setup Wizard will open. You can use it to uninstall the application (see Chapter 19 on pg. 279).

To uninstall the application in the noninteractive mode without restarting the computer (the computer should be restarted manually after uninstalling), enter:

```
msiexec /x <package_name> /qn
```

To uninstall the application in the noninteractive mode and then restart the computer, enter:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

If you opted for password protection against uninstalling the program when you installed the program, you will need to enter the password protection when uninstalling the program. Otherwise program cannot be uninstalled.

To remove the application by entering a password as evidence of the removal privilege, enter:

`msiexec /x <package_name> KLUNINSTPASSWD=******` – to remove application in interactive mode;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – to remove application in non-interactive mode;

CHAPTER 20. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit is a system for centrally managing the key administrative tasks in operating a security system for a company network, based on the applications included in Kaspersky Anti-Virus Business Optimal.

Kaspersky Anti-Virus 6.0 for Windows Workstations is one of the Kaspersky Lab products that can be administered through its own interface, the command line (these methods are described above in this User Guide) or using Kaspersky Administration Kit (if the computer is a part of the centralized remote administration system).

Perform the following steps to manage Kaspersky Anti-Virus 6.0 for Windows Workstations using the Kaspersky Administration Kit:

- deploy *Administration Server* in the network; install Administration *Console* at the administrator's workplace (for more details, see the Administrator Guide for installing Kaspersky Administration Kit 6.0;
- deploy Kaspersky Anti-Virus 6.0 for Windows Workstations and *Administration Agent* (included with Kaspersky Administration Kit) on the network's computers. For more about remote installation of Kaspersky Anti-Virus on network computers, see the Administrator Guide for installing Kaspersky Administration Kit 6.0.

Note the following particulars of using Kaspersky Anti-Virus through Kaspersky Administration Kit:

If computers in the network are have Kaspersky Anti-Virus 5.0 installed, you must take the following steps before upgrading to 6.0 through Kaspersky Administration Kit:

- First, stop the previous version of the application (you can do this remotely through Kaspersky Administration Kit);
- Close all other application before beginning installation;
- Restart the operating system on the remote computer after installation is complete

After upgrading the Kaspersky Lab administration plug-in through Kaspersky Administration Kit, close Administration Console.

Administration Console (see Figure 106) allows you to administer the application through Kaspersky Administration Kit. It provides a standard **MMC-integrated interface** and allows the administrator to perform the following functions:

- remotely install Kaspersky Anti-Virus 6.0 for Windows Workstations and *Administration Agent* on network computers
- remotely configure Kaspersky Anti-Virus on network computers
- update Kaspersky Anti-Virus threat signatures and modules
- manage licenses for the application on network computers
- view information about program operation on client computers

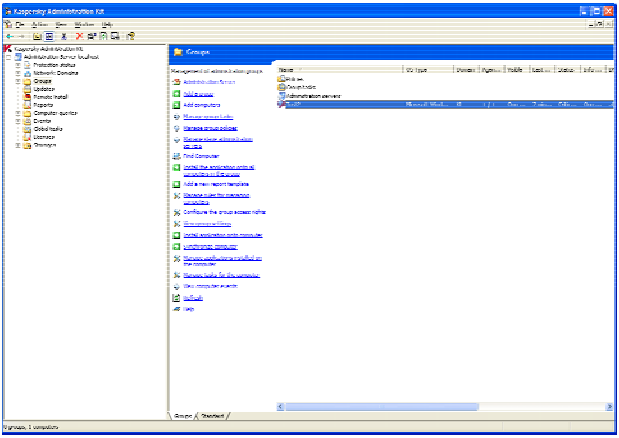


Figure 106. Kaspersky Administration Kit Administration Console

When administering the program centrally through Kaspersky Administration Kit, the administrator determines the settings for policies, tasks, and the application. Protection is designed around these settings.

Application settings are a set of general settings for program operation, including general protection settings, Backup settings, etc.

Task is a specific action performed by the application. Tasks for Kaspersky Anti-Virus 6.0 are divided by type (license key install tasks, on-demand scan tasks, anti-virus database update rollback tasks, anti-virus database and application module update tasks). Each specific task has a set of Kaspersky Anti-Virus settings when performed (*task settings*).

The key feature of centralized administration is grouping remote computers and managing their settings by creating and configuring group policies.

Policy refers to a collection of settings for Kaspersky Anti-Virus operation within a network group. The policy may also include restrictions on modifying the configurations assigned when setting up the application or task.

A policy allows you to manage the complete functionality of the application, since it contains both application settings and settings for all task types, except for settings that must be configured directly when a task starts (for example, task schedules).

20.1. Administering the application

Kaspersky Administration Kit gives you the opportunity to remotely start and pause Kaspersky Anti-Virus on individual client computers, as well as configuring general settings for the application, such as enabling/disabling computer protection, configuring settings for Backup and Quarantine, and configuring settings for creating reports.

To manage application settings:

1. Select the group folder that contains the client computer in the **Groups** folder (see Figure 106).
2. In the result pane, select the computer for which you need to modify application settings. Select the **Applications** command from the context menu or the **Actions** menu.
3. The **Applications** tab in the client computer properties window (see Figure 107) displays a complete list of Kaspersky Lab applications installed on the client computer. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations**.

There are buttons are under the list that you can use to:

- View a list of events in application operation that have occurred on the server and were recorded on the administration server
- View statistical information on application operation
- Configure the application settings (see 20.1.2 on pg. 287)

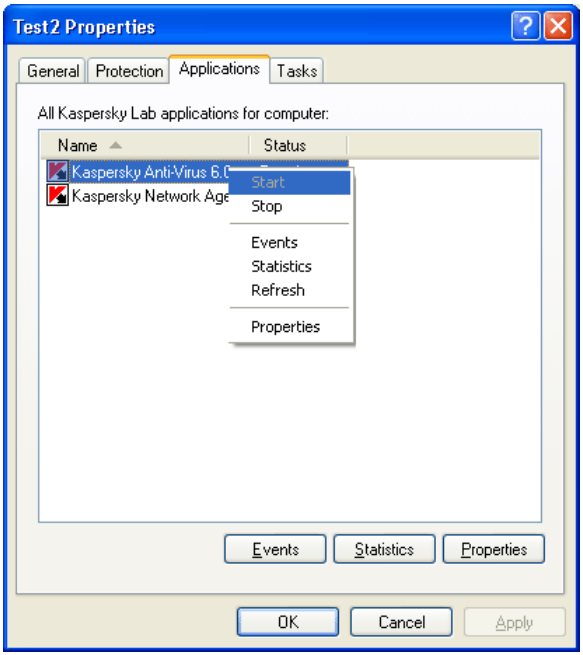


Figure 107. List of Kaspersky Lab applications

20.1.1. Starting/stopping the application

You can start or pause Kaspersky Anti-Virus on a remote computer using the commands from the context menu in the **Computer name Properties** window (see Figure 107).

You can also do this using the **Start/Stop** buttons in the settings window on the **General** tab (see Figure 109).

In the upper part of the window, you will find the name of the application installed, information on the version, the install date, its status (whether the application is running or paused on the local computer), and information about the threat signature database status.

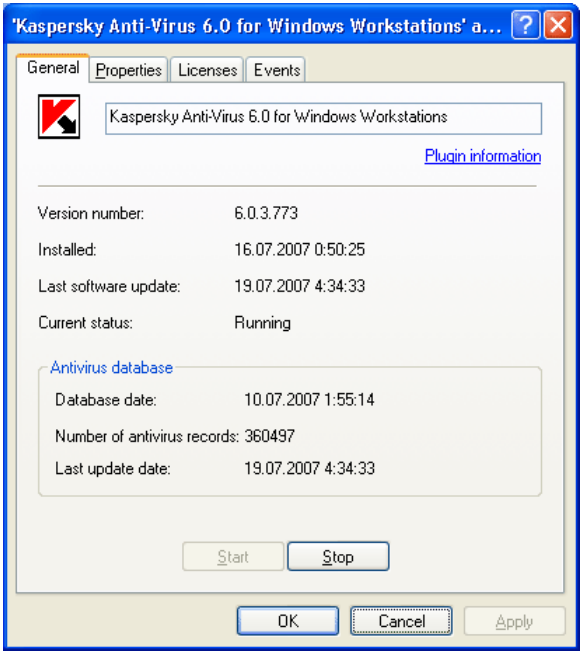


Figure 108. Configuring Kaspersky Anti-Virus settings. **General** tab

20.1.2. Configuring application settings

To view or modify application settings:

1. Open the properties window for the client computer on the **Applications** tab (see Figure 107).
2. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations**. Click the **Properties** button to open the application settings window (see Figure 109).

All the tabs except for the **Properties** tab are standard for Kaspersky Administration Kit. For more on the standard tabs, see the Administrator Guide.

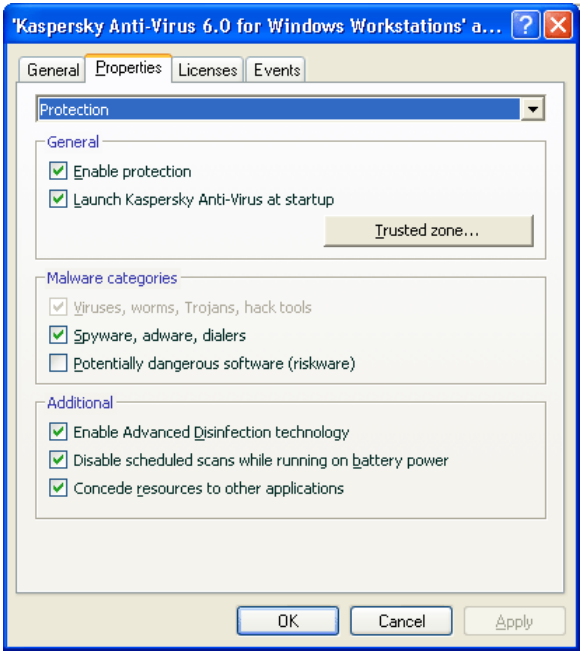


Figure 109. Configuring Kaspersky Anti-Virus settings. **Properties** tab

If a policy has been created for the application (see 20.3.1 on pg. 296) that prevents some settings from being reconfigured, they will not be editable when configuring the application.

On the **Properties** tab, you can configure general protection settings, application protection tools settings, and settings for creating and saving report statistics for the application. To do so, select the needed value from the dropdown menu in the upper portion of the window and configure settings.

Protection
On the **Properties** tab in the **Protection** section, you can: • enable/disable real-time protection for a computer (see 6.1 on pg. 66); • configure automatic startup for the application when the computer is turned on (see 6.1.5 on pg. 70); • create a trusted zone or an exclusion list (see 6.3 on pg. 71);

- select the types of malicious programs that the application will monitor (see 6.2 on pg. 70);
- configure productivity settings for the application and multi-processor configuration settings (see 6.6 on pg. 84).

Service

On the **Properties** tab in the **Service** section, you can:

- Configure notifications for events that occur (see 17.11.1.2 on pg. 257)
- Manage the application's self-defense feature and password protect application settings (see 17.11.1.3 on pg. 258)
- Configure the appearance of the application (see 20.3.1 on pg. 296)
- Configure settings for compatibility between Kaspersky Anti-Virus and other programs (see 17.11.1.3on pg. 258)

Data Files

In this window, you can configure settings for logging statistics on application operation (see 17.3.1 on pg. 227) and specify how long files will be stored in Backup (see 17.1.2 on pg. 221) and Quarantine (see 17.2.2 on pg. 224).

Network Settings

In this window, you can edit the list of ports that Kaspersky Anti-Virus uses for scanning (see 17.7 on pg. 245) and enable/disable SSL scanning (see 17.8 on pg. 247)

20.1.3. Configuring specific settings

When administering Kaspersky Anti-Virus through Kaspersky Administration Kit, you can enable/disable interactivity and edit information on Technical Support. To do so:

1. Open the properties window for the client computer on the **Applications** tab (see Figure 107). Select **Kaspersky Anti-Virus 6.0 for Windows Workstations** and click the **Properties** button. As a result, an application settings window will open.
2. Go to the **Settings** tab (see Figure 108). Select **Service** from the dropdown menu in the upper part of the window.

On the **Service** tab in the **Appearance** window, you can enable/disable Kaspersky Anti-Virus interactivity on a remote computer: displaying the Kaspersky Anti-Virus icon in the system tray, issuing notifications on events that occur in the application (for example, detection of a dangerous object).

If **Enable interface interaction** is checked, a user working on a remote computer will see the Anti-Virus icon and pop-up messages and will have the ability to make decisions on the next steps taken in notification windows regarding events that occur. To disable application interactivity, deselect the checkbox.

On the **Custom support information** tab in the window that opens when you click the **Settings** button, you can edit the information on user technical support that is displayed in the **Service** section of the **Support** item in Kaspersky Anti-Virus (see Figure 97).

To change information in the upper field, enter the current text on the support provided. In the field below, you can edit the hyperlinks that are displayed in the **Technical support online** box that is pulled up when **Support** is selected in the **Service** section.

You can edit the list of sources using the **Add**, **Edit**, and **Delete** buttons. Kaspersky Anti-Virus will add a new link to the top of the list. To change the order of the links in the list, use the **Up**/**Down** buttons.

If the window does not contain any data, the default information on technical support is not subject to editing.

20.2. Managing tasks

This section lists information on managing tasks for Kaspersky Anti-Virus 6.0 for Windows Workstations. For more on the concept of managing tasks through Kaspersky Administration Kit 6.0, see the Administrator Guide for the program.

A list of system tasks is created for each computer when the application is installed. This list (see Figure 110) includes real-time protection tasks (File Anti-Virus, Web Anti-Virus, Mail Anti-Virus, Proactive Defense, Anti-Spy, and Anti-Hacker), virus scan tasks (My Computer, Startup Objects, Critical Areas), and update tasks (threat signature and application module updates and update rollbacks).

> You can start system tasks and configure settings and schedules for them, but they cannot be deleted.

In addition, you can create your own tasks, such as virus scans, application updates and update rollbacks, as well as license key installation tasks (see 20.2.2 on pg. 292).

To view a list of the tasks created for a client computer:

1. Select the group folder that contains the client computer in the **Groups** folder (see Figure 106).

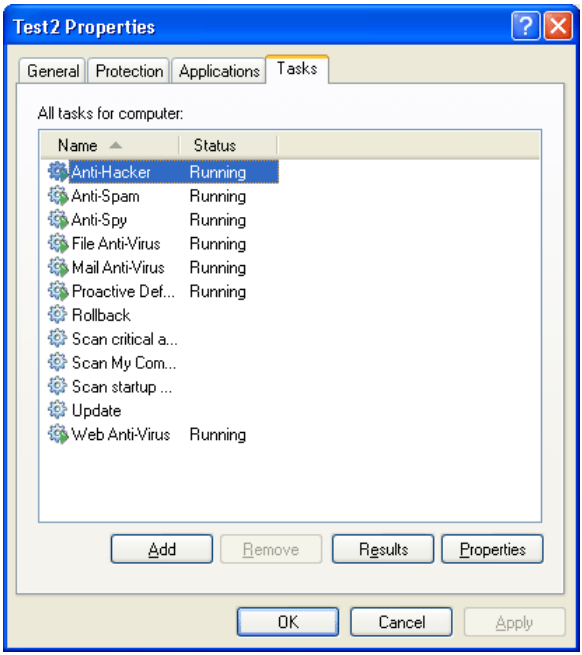


Figure 110. List of application tasks

2. In the result pane, select the computer for which you want to view a list of local tasks. Use the **Tasks** command from the context menu or the same command on the **Actions** menu. Then in the main window a window will open displaying the properties of the client computer.
3. The **Tasks** tab (see Figure 110) displays a complete list of tasks created for that client computer.

20.2.1. Starting and stopping tasks

Tasks are started on the client computer only if the corresponding application is running (see 20.1.1 on pg. 286). If the application is stopped, all tasks started will be terminated.

Tasks are started and paused automatically, according to a schedule, or manually using commands from the context menu and from the View Task Settings window. You can also pause tasks and resume them.

To start/stop/pause/resume a task manually:

Select the necessary task (group or global) from the results pan, open the context menu, and select **Start/Stop/Pause/Resume** or use the same commands on the **Action** menu.

You can initiate the same operations for all task types from the task settings window on the **General** tab (see Figure 111), using the same command buttons.

20.2.2. Creating tasks

When working with the application through Kaspersky Administration Kit, you can create:

- Local tasks, configured for individual computers
- Group tasks, configured for computers joined in one network group
- Global tasks, configured for any set of computers from any network group

You can modify task settings, monitor their performance, copy and move tasks from one group to another, and also delete them using the standard commands **Copy/Paste**, **Cut/Paste**, and **Delete** from the context menu, or the same commands from the **Action** menu.

20.2.2.1. Creating local tasks

To create a local task, take the following steps:

1. Open the local client properties window on the **Tasks** tab (see Figure 110).
2. Click the **Add** button to add a new local task. A task creation wizard will then start up that consists of a series of windows or steps that you can navigate between using the **Back** and **Next** buttons. You complete the wizard by pressing **Finish**. The **Cancel** button will stop the Wizard at any point.

Step 1. Entering general data on the task

The first master window is introductory: here you must specify the name of the task (the **Name** field).

Step 2. Selecting an application and task type

In this step, you must specify the application for which the task is being created (Kaspersky Anti-Virus 6.0 for Windows Workstations). You must also select the task type. The possible tasks for Kaspersky Anti-Virus 6.0 are:

- *Virus scan* – scans for viruses in the areas specified by the user
- *Update* – retrieves and applies update packs for the program
- *Update Rollback* – rolls back to the last program update made
- *License key install* – adds a new license key for using the application

Step 3. Configuring settings for the selected task type

Depending on the task type selected in the previous step, the contents of the following windows can vary:

VIRUS SCAN

The virus scan task configuration window requires you to specify the action Kaspersky Anti-Virus is to take when it detects a dangerous object (see 14.4.4 on pg. 196). You must also create a list of objects to be scanned (see 14.2 on pg. 188).

UPDATE

For threat signature and application module update tasks, you must specify the source that will be used to download updates (see 16.4.1 on pg. 209). The default update source is the Kaspersky Administration Kit update server.

UPDATE ROLLBACK

There are no specific settings for rolling back the most recent update.

INSTALL LICENSE KEY

For license key installation tasks, specify the path to the key file with the **Browse** button. To make an added key a backup, check ☑ **Add as backup key**. The backup license key will become active when the current license key expires.

Information about the key added (license number, type, and expiration date) is displayed in the field below.

Step 4. Selecting a user profile

In this step, you are asked to configure tasks to start under a user account with sufficient privileges to access the object being scanned or update source (for more details, see 6.4on pg. 81).

Step 5. Setting up a schedule

After configuring task settings, you will be asked to configure an automatic task schedule.

To do so, select the frequency for running the task from the dropdown menu and adjust the schedule settings in the lower part of the window.

Step 6. Finishing creating a task

The last window of the wizard will inform you that you have successfully creating a task.

20.2.2.2. Creating group tasks

To create a group task, take the following steps:

1. Select the group for which you want to create a task from the console tree.
2. Select its **Tasks** (see Figure 106) folder, open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu. The task creation wizard will then start, similar to the local task create wizard (for more, see 20.2.2.1 on pg. 292). Follow its instructions.

When the wizard is finished, the task will be added to the **Tasks** folder of that group and all the groups under it, and it will be visible in the results pane.

20.2.2.3. Creating global tasks

To create a global task, take the following steps:

1. Select the **Global tasks** node from the console tree (see Figure 106), open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu.
2. The task creation wizard will then start, similar to the local task create wizard (for more, see 20.2.2.1 on pg. 292). The exception is that there is a stage for creating a list of client computers from the network for which the global task is being created.
3. Select from the network the computers that will run the task. You can select computers from multiple folders or select an entire folder (for more details, see the Administrator Guide for Kaspersky Administration Kit 6.0).

Global tasks are only performed on a selected set of computers. If new client computers are added to a group with computers for which a remote installation task has been created, this task will not run for them. You must create a new task or make corresponding changes to the settings of the existing task.

When the wizard is finished, a global task will be added to the **Global tasks** node of the console tree and will be visible in the results pane.

20.2.3. Configuring specific task settings

To view and modify client computer task settings:

1. Open the properties window for the client computer on the **Tasks** tab (see Figure 110).
2. Select the task from the list and click the **Properties** button. As a result, a task settings window will open (see Figure 111).

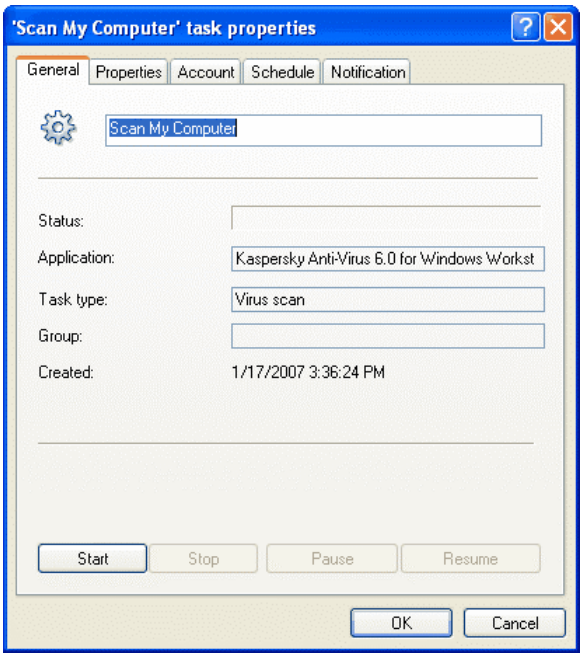


Figure 111. Configuring task settings

All the tabs except for the **Settings** tab are standard for Kaspersky Administration Kit 6.0. They are covered in greater depth in the Administrator

User Guide. The **Settings** tab contains specific settings for Kaspersky Anti-Virus. The contents of this tab vary depending on the task type selected.

Configuration of program task settings through the Kaspersky Administration Kit interface is similar to configuration through the local Kaspersky Anti-Virus interface, with the exception of the settings that are configured individually for each user, such as Anti-Spam white and black lists. See Chapter 7 – Chapter 16 on pp. 86 – 205 of this user guide for a more in-depth description of configuration of task settings.

If a policy has been created for the application (see 20.3 on pg. 296) that blocks some settings from being reconfigured, they will not be editable when configuring tasks.

20.3. Managing policies

Setting up policies allows you to apply universal application and task settings to client computers that belong to a single network group.

This section includes information on creating and configuring policies for Kaspersky Anti-Virus 6.0 for Windows Workstations. For more on the concept of managing tasks through Kaspersky Administration Kit 6.0, see the Administrator Guide for the program.

20.3.1. Creating policies

To create a policy for Kaspersky Anti-Virus, take the following steps:

1. In the **Groups** folder (see Figure 106), select the group of computers for which you need to create a policy.
2. Select **Policies** folder that belongs to the selected group, open the context menu, and use the **Create→Policy** command. A Create New Policy window will appear.

Policies are created in a windows wizard and consists of a series of windows or steps that you can navigate between using the **Back** and **Next** buttons. You finish the wizard by pressing **Finish**. The **Cancel** button will stop the Wizard at any point.

During each step of creating a policy, the settings entered can be locked with the button. If the lock on the button is closed, in the future the values assigned by the policy created will be used when you use the policy on client computers.

Step 1. Entering general data on the policy

The first step of the wizard is introductory. In the first wizard window, you must specify the name of the policy (**Name** field). In the second, select **Kaspersky Anti-Virus 6.0 for Windows Workstations** from the **Application name** dropdown menu. If you want the policy settings to take effect immediately after creating it, check **Make policy active**.

Step 2. Selecting a policy status

This window will ask you to specify the policy status. To do so, move the switch to the need position: active policy or inactive policy.

Several policies may be created in a group for one application, but only one of them can be the current (active) policy.

Step 3. Selecting and configuring protection components

In this stage, you can enable, disable and the configure protection components that will be used in the policy.

All protection components are enabled by default. To disable a component, deselect the textbox next to its name. To fine-tune protection settings or to configure File Anti-Virus, select it from the list and click the **Settings** button.

Step 4. Configuring virus scan settings

In this step, you can configure the settings that will be used by virus scan tasks.

In the **Security level** section, select one of the preset security options (see 14.4.1 on pg. 192). Click the **Settings** button to fine-tune the level selected. To restore the **Recommended** settings, click the **Default** button.

In the **Action** section, specify the action that Anti-Virus should take when a dangerous object is detected (see 14.4.4 on pg. 196).

Step 5. Configuring update settings

In this window, configure settings for the Kaspersky Anti-Virus update distribution feature.

In the **Update settings** section, specify what is being updated (see 16.4.2 on pg. 211). In the window that opens when you click the **Settings** button, assign local network settings (see 16.4.3 on pg. 213) and specify the update source (see 16.4.1 on pg.208).

In the **Actions after updating** section, enable/disable scanning of Quarantine after receiving a new update pack (see 16.4.4 on pg. 215).

Step 6. Enforcing the policy

In this step, select a method for policy enforcement on client computers of the group (for more details, see the Administrator Guide for Kaspersky Administration Kit 6.0).

Step 7. Finishing creating a policy

The final window of the wizard tells you that you have successfully created a policy.

Once the wizard is completed, the Kaspersky Anti-Virus policy will be added to the **Policies** folder (see Figure 106) for the corresponding group and will be visible in the results pane.

You can edit the settings of the policy created and set restrictions on modifying its settings using the button for each settings group. A user on the client computer will not be able to change settings if they are locked this way. The policy will be applied to client computers the first time the clients synchronize with the server.

You can copy or move policies from one group to another and to delete them using the standard commands **Copy**/**Paste**, **Cut**/**Paste**, and **Delete** from the context menu and the same commands from the Action menu.

20.3.2. Viewing and editing policy settings

At the editing stage, you can modify the policy and block modification to settings in nested group policies and in application and task settings.

To view and edit policy settings:

1. Select the computer group for which settings must be edited from the console tree in the **Groups** folder.
2. Select the **Policies** folder that belongs to that group (see Figure 106). When you do so, the results pane will display all the policies created for the group.
3. Select the policy you need from the list of policies for **Kaspersky Anti-Virus 6.0 for Windows Workstations** (the application name is specified in the **Application** field).

4. Select the **Properties** command from the context menu for the selected policy. A policy settings window will open for the application contain several tabs (see Figure 112).

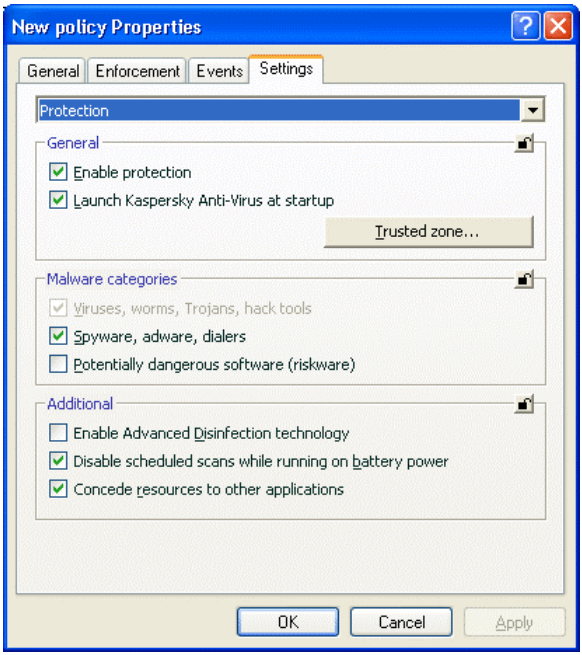


Figure 112. Configuring policy settings

All the tabs except for **Settings** are standard for Kaspersky Administration Kit (for more details, see the Administrator Guide for the program).

The **Settings** tab contains policy settings for Kaspersky Anti-Virus 6.0. Policy settings include program settings (see 20.1.2 on pg. 287) and task settings (see 20.1.3 on pg. 289).

To configure settings, select the needed value from the dropdown menu and configure the settings.

CHAPTER 21. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup and operation of the Kaspersky Anti-Virus for Windows Workstations; here we shall try to answer them here in detail.

Question: Is it possible to use Kaspersky Anti-Virus for Windows Workstations 6.0 with anti-virus products of other vendors?

No. We recommend uninstalling anti-virus products of other vendors prior to installation of Kaspersky Anti-Virus for Windows Workstations to avoid software conflicts.

Question: Kaspersky Anti-Virus for Windows Workstations does not rescan files that have been scanned earlier. Why?

This is true. Kaspersky Anti-Virus for Windows Workstations does not rescan files that have not changed since the last scan.

That has become possible due to new iChecker and iStream technologies. The technology is implemented in the program using a database of file checksums and file checksum storage in alternate NTFS streams.

Question: Why do I need the license key file? Will Kaspersky Anti-Virus for Windows Workstations work without it?

Kaspersky Anti-Virus for Windows Workstations will run without a license key, although you will not be able to access the Updater and Technical Support.

If you still have not decided whether to purchase Kaspersky Anti-Virus for Windows Workstations, we can provide you with a trial license that will work for either two weeks or a month. Once that time has elapsed, the key will expire.

Question: After the installation of Kaspersky Anti-Virus for Windows Workstations the operating system started "behaving" strangely ("blue screen of death", frequent restarting, etc.) What should I do?

Although rare, it is possible that Kaspersky Anti-Virus for Windows Workstations and other software installed on your computer will conflict.

In order to restore the functionality of your operating system do the following:

1. Press the **F8** key repeatedly between the time when the computer just started loading until the boot menu is displayed.
2. Select **Safe Mode** and load the operating system.
3. Open Kaspersky Anti-Virus for Windows Workstations.
4. Use the Settings link in the main window and select the **Protection** section in the program settings window.
5. Uncheck **Launch Kaspersky Anti-Virus 6.0 at startup** and click **OK**.
6. Reboot the operating system in regular mode.

After this contact the Technical Support Service through the Kaspersky Lab's corporate website (**Services→Technical Support)**. Describe in detail the problem and the circumstances in which this problem occurs.

Make sure that you attach to your question a file containing a complete dump of Microsoft Windows operating system. In order to create this file, do the following:

1. Right-click **My computer** and select the **Properties** item in the shortcut menu that will open.
2. Select the **Advanced** tab in the **System Properties** window and then press the **Settings** button in the **Startup and Recovery** section.
3. Select the **Complete memory dump** option from the drop-down list in the **Write debugging information** section of the **Startup and Recovery** window.
4. By default, the dump file will be saved into the system folder as *memory.dmp*. You can change the dump storage folder by editing the folder name in the corresponding field.
5. Reproduce the problem related to the operation of Kaspersky Anti-Virus for Windows Workstations.
6. Make sure that the complete memory dump file was successfully saved.

APPENDIX A. REFERENCE INFORMATION

This appendix contains reference materials on the file formats and extension masks used in Kaspersky Anti-Virus for Windows Workstations settings, and information is also provided on settings in the file setup.ini, which is used when installing the program in hidden mode.

A.1. List of files scanned by extension

If **Scan Programs and Documents (By Extension)** is selected as the File Antivirus scan option or virus scan task, files with the extensions listed below will be analyzed closely for viruses. These file types are also scanned by Mail Anti-Virus if message attachment scanning is activated:

com – executable file for a program

exe – executable file or self-extracting archive

sys – system driver

prg – program text for dBase, Clipper or Microsoft Visual FoxPro, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a .bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic loading library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program that runs in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – initialization file

cla – Java class

vbs – Visual Basic script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML with built-in PHP scripts

php – script built into HTML files

wsh – Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper

hlp – Win Help file

eml – Microsoft Outlook Express email file

nws – Microsoft Outlook Express new email file

msg – Microsoft Mail email file

plg – email

mbx – extension for saved Microsoft Office Outlook emails

*doc** – a Microsoft Word document, such as: *doc* – a Microsoft Word document, *docx* – a Microsoft Word 2007 document with XML support, *docm* – a Microsoft Word 2007 document with Macro support

*dot** – a Microsoft Word document template, such as, *dot* – a Microsoft Word document template, *dotx* – a Microsoft Word 2007 document template, *dotm* – a Microsoft Word 2007 document template with Macro support

fpm – database program, start file for Microsoft Visual FoxPro

rtf – Rich Text Format document

shs – Shell Scrap Object Handler fragment

dwg – AutoCAD blueprint database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave Flash file

jpg, jpeg, png – compressed image graphics format

emf – Enhanced Metafile format Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows

ico – icon file

ov? – Microsoft DOC executable files

*xl** – – Microsoft Office Excel documents and files, such as: *xla* - Microsoft Office Excel extension, *xlc* - diagram, *xlt* - document templates. *xlsx* – a Microsoft Excel 2007 workbook, *xltm* – a Microsoft Excel 2007 workbook with Macro support, *xlsb* – a Microsoft Excel 2007 in binary (non-XML) format, *xltx* – a Microsoft Excel 2007 template, *xlsm* – a Microsoft Excel 2007 template with Macro support, *xlam* – a Microsoft Excel 2007 plugin with Macro support.

*pp** – Microsoft Office Excel documents and files, such as: *xla* - Microsoft Office Excel extension, *xlc* - diagram, *xlt* - document templates. *xlsx* – a Microsoft Excel 2007 workbook, *xltm* – a Microsoft Excel 2007 workbook with Macro support, *xlsb* – a Microsoft Excel 2007 in binary (non-XML) format, *xltx* – a Microsoft Excel 2007 template, *xlsm* – a Microsoft Excel 2007 template with Macro support, *xlam* – a Microsoft Excel 2007 plugin with Macro support.

*md** – Microsoft Office Access documents and files, such as: *mda* – Microsoft Office Access work group, mdb – database, etc.

sldx – a Microsoft PowerPoint 2007 slide.

sldm – a Microsoft PowerPoint 2007 slide with Macro support.

thmx – a Microsoft Office 2007 theme.

Remember that the actual format of a file may not correspond with the format indicated in the file extension.

A.2. Possible file exclusion masks

Let's look at some examples of possible masks that you can use when creating file exclusion lists:

- Masks without file paths:
  - ***.exe** – all files with the extension *.exe*
  - ***.ex?** – all files with the extension *.ex?*, where ? can represent any one character
  - **test** – all files with the name *test*
- Masks with absolute file paths:
  - **C:\dir*.*** or **C:\dir*** or **C:\dir** – all files in folder *C:\dir*

- **C:\dir*.exe** – all files with extension .exe in folder *C:\dir*
- **C:\dir*.ex?** – all files with extension .ex? in folder *C:\dir*, where ? can represent any one character
- **C:\dir\test** – only the file *C:\dir\test*

If you do not want the program to scan files in the subfolders of this folder, uncheck **Include subfolders** when creating the mask.

- Masks with relative file paths:
  - **dir*.*** or **dir*** or **dir** – all files in all *dir* folders
  - **dir\test** – all *test* files in *dir\ folders*
  - **dir*.exe** – all files with the extension *.exe* in all *dir\ folders*
  - **dir*.ex?** – all files with the extension .ex? in all *C:\dir* folders, where ? can represent any one character

If you do not want the program to scan files in the subfolders of this folder, uncheck **Include subfolders** when creating the mask.

Tip:

. and * exclusion masks can only be used if you assign a verdict excluded according to the Virus Encyclopedia. Otherwise the threat specified will not be detected in any objects. Using these masks without selecting a verdict essentially disables monitoring.

We also do not recommend that you select a virtual drive created on the basis of a file system directory using the *subst* command as an exclusion. There is no point in doing so, since during the scan, the program perceives this virtual drive as a folder and consequently scans it.

A.3. Possible threat exclusion masks

When adding threats with a certain verdict from the Virus Encyclopedia classification as exclusions, you can specify:

- the full name of the threat as given in the Virus Encyclopedia at www.viruslist.com (for example, **not-a-virus:RiskWare.RemoteAdmin.RA.311** or **Flooder.Win32.Fuxx**);
- threat name by mask. For example:

- **not-a-virus*** – excludes potential dangerous programs from the scan, as well as joke programs.
- ***Riskware.*** – excludes riskware from the scan.
- ***RemoteAdmin.*** – excludes all remote administration programs from the scan.

A.4. Overview of settings in *setup.ini*

The file *setup.ini*, located in the Kaspersky Anti-Virus installation folder, is used when installing the program in noninteractive mode from the command prompt (see 3.3 on pg. 44) or using Group Policy Object Editor (see 3.4 on pg.45). The file contains the following settings :

[Setup] – general settings for program installation.

InstallDir=<path to program installation folder>.

Reboot=yes|no – whether the computer should restart after the program is installed (does not restart by default).

SelfProtection=yes|no – whether Kaspersky Anti-Virus should enable Self-Defense during installation (enabled by default).

[Components] – selects the components to install. If no components are specified, all will be installed. If any components are specified, the components that are not listed are not installed.

FileMonitor=yes|no – installs File Anti-Virus

MailMonitor=yes|no – installs Mail Anti-Virus

WebMonitor=yes|no – installs Web Anti-Virus

ProactiveDefence=yes|no – installs Proactive Defense

AntiSpy=yes|no – installs Anti-Spy

AntiHacker=yes|no – installs Anti-Hacker

AntiSpam=yes|no – installs Anti-Spam

[Tasks] – enables Kaspersky Anti-Virus tasks If no tasks are specified, all tasks will run after installation. If any tasks are specified, all tasks that are not listed will be disabled.

ScanMyComputer=yes|no – task for complete scan of computer

ScanStartup=yes|no – task for scanning startup objects

ScanCritical=yes|no – task for scanning critical areas

Updater=yes|no – task for updating threat signatures and program modules

Instead of the value **yes**, you can use the values **1**, **on**, **enable**, or **enabled**, and instead of **no** you can use – **0**, **off**, **disable**, or **disabled**.

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, email systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

B.1. Other Kaspersky Lab Products

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, notifications about the current status of virus activity, and fresh news. The program reads the list of available news feeds and their content from the Kaspersky Lab news server at specified intervals.

News Agent enables users to;

- See the current virus forecast in the system tray
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

News Agent is a stand-alone Microsoft Windows application that can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infectionson their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky® OnLine Scanner Pro

The program is a subscription service available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning

- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks, including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used, as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, folders, or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Controls modifications within the file system**. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitors processes in random-access memory**. Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.
- **Monitors changes in OS registry** due to internal system registry control.
- **Hidden Processes Monitor** helps protect from malicious code concealed in the operating system using rootkit technologies.
- **Heuristic Analyzer**. When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.
- **Performs system restore** after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection**: anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.
- **Proactive protection**: the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity. *Privacy Control* module keeps your confidential information secure from unauthorized access and transmission. *Parental Control* is a Kaspersky Internet Security component that monitors user access to the Internet.

Kaspersky Internet Security 7.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical network attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth Mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body
- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program provides comprehensive virus scanning, including:

- **On-demand scans** of the mobile device's onboard memory, memory cards, an individual folder, or a specific file; if an infected file is detected, it is moved to Quarantine or deleted
- **Real-time scanning –** all incoming and outgoing files are automatically scanned, as well as files when attempts are made to access them
- **Protection from text message spam**

Kaspersky Anti-Virus for File Servers

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Features and functionality:

- *Protects server file systems in real time: All server files are scanned when opened or saved on the server*
- *Prevents virus outbreaks;*
- *On-demand scans of the entire file system or individual files and folders;*
- *Use of optimization technologies when scanning objects in the server file system;*
- *System rollback after virus attacks;*

- *Scalability of the software package within the scope of system resources available;*
- *Monitoring of the system load balance;*
- *Creating a list of trusted processes whose activity on the server is not subject to control by the software package;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Saving backup copies of infected and deleted objects in case you need to restore them;*
- *Quarantining suspicious objects*;
- *Send notifications on events in program operation to the system administrator;*
- *Log detailed reports*;
- *Automatically update* program databases.

Kaspersky Open Space Security

Kaspersky Open Space Security is a software package withal new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

Kaspersky WorkSpace Security is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam*;
- *Proactive Defense from new malicious programs whose signatures are not yet added to the database;*

- *Personal Firewall with intrusion detection system and network attack warnings;*
- *Rollback for malicious system modifications*;
- *Protection from phishing attacks and junk mail*;
- *Dynamic resource redistribution* during complete system scans;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco® NAC* (Network Admission Control);
- *Scanning of e-mail and Internet traffic* in real time;
- *Blocking of popup windows and banner ads* when *on the Internet;*
- *Secure operation in any type of network*, including Wi-Fi;
- *Rescue disk creation tools that enable you to restore your system after a virus outbreak;*
- *An extensive reporting system* on protection status;
- *Automatic database updates*;
- *Full support for 64-bit operating systems*;
- *Optimization of program performance on laptops* (Intel® Centrino® Duo technology);
- *Remote disinfection capability* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- Remote administration of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco® NAC* (Network Admission Control);
- *Protection of workstations and file servers from all types of Internet threats*;
- *iSwift technology to avoid rescanning files within the network*;

- *Distribution of load among server processors*;
- *Quarantining suspicious objects* from workstations;
- *Rollback for malicious system modifications*;
- *scalability of the software package within the* scope of system resources available;
- *Proactive Defense* for workstations from new malicious programs whose signatures are not yet added to the database;
- *Scanning of e-mail and Internet traffic* in real time;
- *Personal Firewall* with intrusion detection system and network attack warnings;
- *Protection while using* Wi-Fi networks;
- *Self-Defense from malicious programs*;
- *Quarantining* suspicious objects;
- *automatic database updates*.

Kaspersky Enterprise Space Security

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- *Protection of workstations and file servers from viruses, Trojans, and worms*;
- *Protection of Sendmail, Qmail, Postfix and Exim mail servers*;
- *Scanning of all e-mails on Microsoft Exchange Server*, including shared folders;
- *Processing of e-mails, databases, and other objects for Lotus Domino servers*;
- *Protection from phishing attacks and junk mail*;
- *preventing mass mailings and virus outbreaks*;
- scalability of the software package within the scope of system resources available ;
- *Remote administration of the software package, including centralized installation, configuration, and administration;*

- *Support for Cisco ® NAC (Network Admission Control);*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation while using* Wi-Fi networks;
- *Scans Internet traffic* in real time;
- *Rollback for malicious system modifications*;
- *Dynamic resource redistribution* during complete system scans;
- Quarantining suspicious objects ;
- *An extensive reporting system* on protection system status;
- *automatic database updates*.

Kaspersky Total Space Security

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam* on all levels of the corporate network, from workstations to Internet gateways;
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database* ;
- *Protection of mail servers and linked servers*;
- *Scans Internet traffic* (HTTP/FTP) entering the local area network in real time;
- scalability of the software package within the scope of system resources available ;
- *Blocking access from infected workstations*;
- *Prevents virus outbreaks*;
- *Centralized reporting on protection status*;

- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC* (Network Admission Control);
- *Support for hardware proxy servers*;
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *iSwift technology to avoid rescanning files within* the network ;
- *Dynamic resource redistribution during complete system scans;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation for users on any type of network*, including Wi-Fi;
- *Protection from phishing attacks and junk mail*;
- *Remote disinfection capability* (Intel® Active Management, Intel® vPro™);
- *Rollback for malicious system modifications*;
- *Self-Defense from malicious programs*;
- *full support for 64-bit operating systems*;
- *automatic database updates*.

Kaspersky Security for Mail Servers

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs*;
- *Junk mail filtering*;
- *Scans incoming and outgoing e-mails and attachments*;
- *Scans all e-mails on* Microsoft Exchange Server for viruses, including shared folders;
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers*;
- *Filters* e-mails by attachment type;
- *Quarantines* suspicious objects;
- *Easy-to-use administration system for* the program;
- *Prevents virus outbreaks*;
- *Monitors protection system status* using notifications;
- *Reporting system* for program operation;
- scalability of the software package within the scope of system resources available ;
- *automatic database updates*.

Kaspersky Security for Internet Gateways

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs*;
- *Scans Internet traffic* (HTTP/FTP) in real time;
- *Filters Internet traffic* using a trusted server list, object types, and user groups;
- *Quarantines* suspicious objects;
- *Easy-to-use administration system*;

- *Reporting system for program operation*;
- *Support for hardware proxy servers*;
- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates*.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database, adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic in real time.

B.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: info@kaspersky.com

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS WORKSTATIONS (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD’S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD’s SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

1. *License Grant*. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby

grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes.

1.1 *Use*. The number of computers that User may protect by the Software is specified in the License Key File and indicated in the "Service" window. The Software may not be used to protect any networks with more than this number of computers.

1.1.1 The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses and network attacks whose signatures are contained in the threat signatures and network attacks databases which are available on Kaspersky Lab's update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.8 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.9 Removal of Potentially Harmful Products. You acknowledge and agree that, in addition to detecting harmful and malicious software, the Product may also identify, remove and/or disable potentially harmful products, including those that are regarded or classified as Adware, Riskware, Pornware etc.

2. *Support*.

1. Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:

   (a) payment of its then current support charge, and:

   (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

   (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders assistance in Software activation and registration of the End User only.

2. By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

3. Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

4. "Support Services" means:

   - Hourly updates of the anti-virus database;
   - Updates of network attacks database;
   - Updates of anti-spam database;

   I. Free software updates, including version upgrades;

   II. Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

   III. Virus detection and disinfection updates in 24-hours period.

5. Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the

official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights*. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality*. You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the activation code.

5. *Limited Warranty*.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses and spam letters, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))

(v) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(vi) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b)

use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vii) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability*.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).